THREAT MODELING · OSTERING.COM · VERSION 1.0 · 4 NOVEMBER 2026

Hospital and Medical Device Threat Taxonomy

This is the reference for the Critical Condition card game: every card's threat, the mitigation principle a sound design follows, design measures, and mappings to STRIDE, LINDDUN, CAPEC, CWE, ATT&CK, EMB3D and MDS2.

What is in it

231 entries: 221 threats in 17 suits across two decks, The Patient (8 suits) and The Hospital (9 suits), plus 10 structural hazards played as Trumps in both decks.

Each entry gives the threat, the three prompts printed on its card, the mitigation principle, design measures and mappings. Every ID is the one printed on the card.

`https://ostering.com/taxonomies/hospitals-and-medical-devices/`

Licence

CC BY-NC-ND 4.0, with additional permissions: share it unchanged, with credit, for non-commercial use; threat model with it, including for clients; ask before shipping it in a product.

The full terms are on the Licence page and at `https://ostering.com/taxonomies/hospitals-and-medical-devices/#licence`.

© 2026 Jonathan Brett Crawley. Critical Condition · Created by Brett Crawley.

How to read it

Each entry

ID. Game prefix, suit and rank joined by hyphens, for example `CRI-PM-K` or `CRI-TR-4`. The hyphens make each ID one searchable token. Ranks are frozen: an entry added later takes an intermediate rank, such as `CRI-PM-3.1`, so no published ID changes.

Threat. The design weakness and what it leads to, written against the system under review.

Mitigation prompts. The three questions printed on the card, for the table to answer about its own design.

Mitigation principle and design measures. The principle a sound design follows, then three or four concrete measures. Other designs can meet the principle in other ways.

† **Direct harm** marks a threat that can physically injure or kill a patient. † **Care delayed or wrong** marks harm through wrong or delayed treatment. In a game, a red † is not accepted without the person who owns clinical safety for the system, and an amber † needs a clinical lead's sign-off.

Mappings

STRIDE; LINDDUN where there is a privacy angle; CAPEC 3.9; CWE 5.0 (28 October 2026); MITRE ATT&CK v20.0 (Enterprise, and ICS for T0 techniques); MITRE EMB3D for embedded devices; the MDS2 (ANSI/NEMA HN 1-2019) security capabilities that counter the threat, main one first; and the standards that address the entry directly. Every ID was checked against the publisher's data, with revoked and deprecated entries and Discouraged or Prohibited CWEs excluded. A blank means nothing fitted well, because a loose tag would mislead.

Also as Excel, SKOS (JSON-LD) and STIX 2.1 from the overview page.

The suits

ID	Suit	Deck	Entries	Page under /taxonomies/hospitals-and-medical-devices/
CRI-IM	**Implants and Programmers** · Pacemakers, ICDs, neurostimulators, cochlear and retinal implants and implantable pumps, with the programmers, home transmitters and clouds that talk to them.	The Patient	13	implants-and-programmers/
CRI-BW	**Body-worn and Home-use Devices** · Insulin pumps, CGMs and closed loops, patch and Holter ECG, pulse oximeters, BP cuffs, hearing aids and connected inhalers, and the phones that control them.	The Patient	13	body-worn-and-home-use-devices/
CRI-PM	**Patient Monitoring** · Bedside monitors (ECG, SpO2, NIBP and invasive BP, heart rate, respiration, capnography, temperature), central stations, telemetry and early-warning feeds.	The Patient	13	patient-monitoring/
CRI-LS	**Life Support and Therapy** · Ventilators and respirators, anaesthesia workstations, oxygen, defibrillators, dialysis, ECMO, neonatal incubators and surgical robots.	The Patient	13	life-support-and-therapy/
CRI-MD	**Medication Delivery** · Infusion and PCA pumps, drug libraries, pump-EHR auto-programming, barcode administration, dispensing cabinets, pharmacy robots and controlled drug records.	The Patient	13	medication-delivery/
CRI-IR	**Imaging and Radiation** · X-ray, CT, MRI, fluoroscopy, ultrasound, mammography, nuclear medicine and radiotherapy, with their worklists, workstations, images and dose.	The Patient	13	imaging-and-radiation/
CRI-LD	**Laboratory and Diagnostics** · Analysers, LIS and middleware, point-of-care tests, blood bank, pathology and digital pathology, sequencers and outsourced lab services.	The Patient	13	laboratory-and-diagnostics/
CRI-CA	**Clinical Software and AI** · Software as a medical device, decision support, dose calculators, early-warning and sepsis scores, imaging AI, AI scribes and the apps clinicians reach for.	The Patient	13	clinical-software-and-ai/
CRI-RC	**Records and Patient Data** · The EHR and patient administration, orders and results, identity matching, sensitive categories, portals, research use and the audit trail.	The Hospital	13	records-and-patient-data/
CRI-IN	**Integration and Interoperability** · HL7 v2, FHIR, DICOM, integration engines, device integration middleware and regional exchange.	The Hospital	13	integration-and-interoperability/
CRI-NW	**Networks and Wireless** · Segmentation, legacy systems inside devices, Wi-Fi, WMTS telemetry, Bluetooth, RTLS, device inventory and satellite sites.	The Hospital	13	networks-and-wireless/
CRI-CC	**Clinical Communications** · Nurse call, alarm routing to handsets, pagers and bleeps, DECT and Wi-Fi phones, secure and shadow messaging, crash calls, switchboard and overhead paging.	The Hospital	13	clinical-communications/
CRI-EC	**Emergency and External Communications** · Ambulance dispatch, prehospital ECG and pre-alerts, emergency services radio, diversion, image transfer, telehealth, hospital-at-home hubs, staff call-in, patient SMS and backup links.	The Hospital	13	emergency-and-external-communications/
CRI-FB	**Facilities and Building Systems** · Medical gases, theatre and isolation ventilation, backup power, cold storage, water, sterile services, pneumatic tubes, lifts, infant security and building management.	The Hospital	13	facilities-and-building-systems/

CRI-SV	**Suppliers, Service and Lifecycle** · Vendor remote service, service laptops, manufacturer clouds, patching rights, end of support, procurement evidence, refurbished devices, disposal and vendor failure.	The Hospital	13	`suppliers-service-and-lifecycle/`
CRI-AC	**Identity and Access** · Clinician identities, default and hard-coded credentials, shared directories, shared logins, break-glass, session handover, privileged and temporary accounts, badges.	The Hospital	13	`identity-and-access/`
CRI-CD	**Continuity and Downtime** · Estate-wide ransomware, shared services, backups, restore validation, downtime procedures and copies, diversion, incident communications and extortion.	The Hospital	13	`continuity-and-downtime/`
CRI-TR	**Structural hazards** · Ten structural hazards of hospitals and medical devices as a whole. Both decks carry them, ranked 1 (highest) to 10.	Both decks	10	`structural-hazards/`

Licence

© 2026 Jonathan Brett Crawley. This taxonomy is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International licence (CC BY-NC-ND 4.0), with the additional permissions below. You can share the whole taxonomy freely for non-commercial purposes, unchanged and with credit.

Use	Permission needed?
Sharing the whole taxonomy non-commercially (OWASP, universities, conferences, individuals)	No
Threat modeling with it, including for paying clients	No
Internal use and training inside any organisation	No
Quoting entries, with credit, in paid courses, reports and talks	No
Shipping the taxonomy in a product: a tool's built-in library, a printed deck, a reprint for sale	Yes, ask me

Additional permissions. In addition to the rights the licence gives, and whether or not the use is commercial, the copyright holder grants you permission to:

- use the taxonomy to threat model systems you build, operate or assess, including for paying clients;
- use it internally, and for training, inside any organisation;
- quote individual entries, with credit, in paid courses, reports, findings and talks.

Any other commercial use, including shipping the taxonomy or a substantial part of it in a product (a tool's built-in library, a printed deck, a reprint for sale), needs written permission. Ask me on LinkedIn.

Credit: “Hospital and Medical Device Threat Taxonomy” by Jonathan Brett Crawley, ostering.com, licensed under CC BY-NC-ND 4.0.

These additional permissions are given alongside the licence. They add to what the licence allows and do not take anything away from it.

Licence text: https://creativecommons.org/licenses/by-nc-nd/4.0/

CRI-IM · THE PATIENT · 13 ENTRIES

Implants and Programmers

Pacemakers, ICDs, neurostimulators, cochlear and retinal implants and implantable pumps, with the programmers, home transmitters and clouds that talk to them.

https://ostering.com/taxonomies/hospitals-and-medical-devices/implants-and-programmers/

CRI-IM-A Unauthenticated therapy commands over the air

† DIRECT HARM THE PATIENT · RANK A

THREAT

The implant accepts programming commands over its radio link without proving the programmer is genuine. Anyone within range with a suitable transmitter could change pacing, stop therapy or deliver a shock.

MITIGATION PROMPTS (ON THE CARD)

1. How does the implant know the programmer talking to it is genuine?
2. Which therapy changes can be made over the radio link at all?
3. What stops a nearby transmitter injecting a programming command?

SEEN IN PUBLIC

Medtronic Conexus telemetry, 2019. US government advisories warned that the Conexus radio protocol used by Medtronic implantable defibrillators, clinic programmers and home monitors had no authentication or encryption, so someone nearby could read or change device settings. Sources: CISA: ICS Medical Advisory ICSMA-19-080-01

MITIGATION PRINCIPLE

An implant acts only on commands from a programmer it has authenticated, over a link protected for integrity.

DESIGN MEASURES

1. Require mutual authentication between implant and programmer before any therapy-changing command is accepted.
2. Protect every command with message integrity and freshness so injected or altered commands are rejected.
3. Limit the commands available over long-range radio; keep therapy changes to close-range sessions.
4. Log every programming session in the implant for review at the next follow-up.

MAPPINGS

STRIDE	S Spoofing, T Tampering, E Elevation of privilege
CAPEC	CAPEC-594 Traffic Injection CAPEC-216 Communication Channel Manipulation
CWE	CWE-306 Missing Authentication for Critical Functionality CWE-940 Improper Verification of Source of a Communication Channel
ATT&CK	T0831 Manipulation of Control
EMB3D	TID-406 Unauthorized Messages or Connections TID-310 Remotely Accessible Unauthenticated Services
MDS2	NAUT Node authentication, AUTH Authorization, TXIG Transmission integrity
Standards	FDA premarket AAMI SW96 ISO 14971

CRI-IM-K Malicious firmware loaded into the body

† DIRECT HARM THE PATIENT · RANK K

THREAT

Firmware for the implant can be installed from a programmer or home transmitter without verifying who signed it. A modified build changes therapy or bricks the device, and the only recovery is surgery to replace it.

MITIGATION PROMPTS (ON THE CARD)

1. Who signs implant firmware, and where does the implant check it?
2. Can an older, weaker firmware version be installed again?
3. What happens to therapy if an update fails part way?

SEEN IN PUBLIC

Abbott (St. Jude Medical) pacemakers, 2017. The FDA approved a firmware update for about 465,000 radio-enabled Abbott pacemakers in the US to stop unauthorised reprogramming; patients had to visit a clinic to have it applied, weighing a small risk of update failure. Sources: Help Net Security: Patients with St. Jude pacemakers called in for firmware update; CSO: 465,000 Abbott pacemakers vulnerable to hacking need a firmware fix

MITIGATION PRINCIPLE

Implant firmware is accepted only when signed by the manufacturer and is never allowed to roll back to a weaker version.

DESIGN MEASURES

1. Verify a manufacturer signature in the implant before installing any firmware, whatever channel delivered it.
2. Refuse rollback to earlier firmware with known vulnerabilities.
3. Keep a protected fallback image and safe therapy mode if an update fails or is interrupted.
4. Restrict firmware installation to in-clinic sessions with a clinician present unless risk analysis justifies remote delivery.

MAPPINGS

STRIDE	T Tampering, E Elevation of privilege, D Denial of service
CAPEC	CAPEC-186 Malicious Software Update CAPEC-669 Alteration of a Software Update
CWE	CWE-494 Download of Code Without Integrity Check CWE-347 Improper Verification of Cryptographic Signature
ATT&CK	T1495 Firmware Corruption
EMB3D	TID-211 Device Allows Unauthenticated Firmware Installation TID-213 Faulty FW/SW Update Integrity Verification TID-216 Firmware Update Rollbacks Allowed
MDS2	IGAU Health data integrity and authenticity, CSUP Cybersecurity product upgrades
Standards	FDA premarket IEC 81001-5-1

CRI-IM-Q Remote monitoring cloud controls thousands

† DIRECT HARM THE PATIENT · RANK Q

THREAT

Home transmitters link implants to the manufacturer's cloud for follow-up and updates. If that cloud or its update path is compromised, an attacker reaches every connected patient at once: harvesting their data, altering transmitters or pushing changes towards implants.

MITIGATION PROMPTS (ON THE CARD)

1. What can the monitoring cloud actually change in a patient's implant?
2. How many patients would one cloud compromise reach?
3. Who reviews changes pushed to home transmitters before release?

MITIGATION PRINCIPLE

A compromise of the remote monitoring service cannot change therapy in the body or reach all patients at once.

DESIGN MEASURES

1. Never let the cloud issue therapy changes; reserve them for authenticated clinician sessions.
2. Sign transmitter updates offline and verify them on the transmitter, so cloud compromise alone cannot push code.
3. Segment the service by region and clinic, and rate-limit any fleet-wide action with human approval.
4. Encrypt implant data end to end from transmitter to the clinic, not only to the cloud.

MAPPINGS

STRIDE	S Spoofing, T Tampering, I Information disclosure, E Elevation of privilege
LINDDUN	DD Data disclosure, L Linking
CAPEC	CAPEC-187 Malicious Automated Software Update via Redirection CAPEC-439 Manipulation During Distribution
CWE	CWE-940 Improper Verification of Source of a Communication Channel CWE-1357 Reliance on Insufficiently Trustworthy Component
ATT&CK	T1199 Trusted Relationship T1195.002 Compromise Software Supply Chain
EMB3D	TID-303 Excessive Trust in Offboard Management/IDE Software
MDS2	RMOT Remote service, NAUT Node authentication, CONN Connectivity capabilities
Standards	IEC 81001-5-1 FDA premarket

CRI-IM-J Locked out in an emergency

† DIRECT HARM THE PATIENT · RANK J

THREAT

Locking the implant to authenticated programmers can stop an emergency team reading or adjusting it for an unconscious patient far from their clinic. Leaving it open to any programmer instead leaves it open to anyone. Either design can harm the patient.

MITIGATION PROMPTS (ON THE CARD)

1. How does an emergency team read this implant far from its clinic?
2. What can emergency access change, and for how long?
3. Where is an emergency session recorded, and who reviews it?

MITIGATION PRINCIPLE

Emergency access is a deliberate, narrow and logged path, designed with clinicians, not a side effect of weak authentication.

DESIGN MEASURES

1. Provide an emergency mode that needs close physical proximity, such as an inductive or magnet trigger, and expires quickly.
2. Limit emergency mode to reading status and applying safe therapy settings.
3. Record every emergency session in the implant and report it at the next follow-up.
4. Give patients an ID card and publish the emergency procedure for emergency departments worldwide.

MAPPINGS

STRIDE	S Spoofing, E Elevation of privilege, D Denial of service
CAPEC	CAPEC-115 Authentication Bypass
CWE	CWE-636 Not Failing Securely
MDS2	EMRG Emergency access, AUDT Audit controls, PAUT Person authentication
Standards	ISO 14971 AAMI SW96

CRI-IM-10 Replayed programming sessions

† DIRECT HARM THE PATIENT · RANK 10

THREAT

Programming messages carry no freshness check, so a recorded session can be played back later. A therapy change the patient once needed is reapplied when it is no longer safe, or a reset is repeated.

MITIGATION PROMPTS (ON THE CARD)

1. What makes each programming command unusable a second time?
2. How is a command tied to one programming session?
3. Would the implant notice a recorded session played back next week?

MITIGATION PRINCIPLE

Every programming command is fresh, bound to one session and useless if replayed.

DESIGN MEASURES

1. Bind commands to a session key agreed at the start of each authenticated session.
2. Use counters or nonces so the implant rejects any message it has already processed.
3. Expire sessions on a short timer and when the programmer moves out of range.

MAPPINGS

STRIDE	S Spoofing, T Tampering
CAPEC	CAPEC-94 Adversary in the Middle (AiTM)
CWE	CWE-294 Authentication Bypass by Capture-replay
ATT&CK	T0830 Adversary-in-the-Middle
EMB3D	TID-407 Missing Message Replay Protection TID-221 Authentication Bypass By Message Replay
MDS2	TXIG Transmission integrity, NAUT Node authentication
Standards	FDA premarket

CRI-IM-9 Magnet and test modes as backdoors

† DIRECT HARM THE PATIENT · RANK 9

THREAT

Magnet modes, factory test commands and undocumented engineering functions stay reachable in released implants. They suspend shocks, force fixed-rate pacing or expose memory without any electronic authentication, and few clinicians know they exist.

MITIGATION PROMPTS (ON THE CARD)

1. Which magnet, test or engineering modes remain in the released implant?
2. Who knows these modes exist, and are they documented for clinicians?
3. Can any of these modes be triggered without authentication?

MITIGATION PRINCIPLE

Every mode that changes therapy is documented, intended for clinical use and controlled; nothing from manufacturing survives in release.

DESIGN MEASURES

1. Remove or permanently lock factory test and debug commands before implantation.
2. Document every magnet and special mode and its clinical effect in the labelling.
3. Log entry into special modes and show it at the next interrogation.
4. Test released firmware for undocumented commands as part of security verification.

MAPPINGS

STRIDE	T Tampering, E Elevation of privilege
CAPEC	CAPEC-36 Using Unpublished Interfaces or Functionality CAPEC-121 Exploit Non-Production Interfaces
CWE	CWE-912 Hidden Functionality CWE-1269 Product Released in Non-Release Configuration
ATT&CK	T0858 Change Operating Mode
EMB3D	TID-224 Excessive Access via Software Diagnostic Features TID-401 Undocumented Protocol Features
MDS2	SAHD System and application hardening, AUDT Audit controls
Standards	FDA premarket AAMI SW96

CRI-IM-8 Abandoned implants

† CARE DELAYED OR WRONG · THE PATIENT · RANK 8

THREAT

The manufacturer leaves the market, is sold or stops supporting a product. Patients keep an implant that no clinic can program, no one patches and no one answers for, and replacing it means surgery.

MITIGATION PROMPTS (ON THE CARD)

1. Who programs and patches this implant if the maker stops supporting it?
2. Is support promised for the full life of the patient's device?
3. What would patients and clinics be told if the product were withdrawn?

SEEN IN PUBLIC

Argus II retinal implant, 2020. Second Sight phased out its Argus II retinal implant and, after laying off most staff in March 2020, could no longer support its more than 350 recipients; patients were left with implants that could not be repaired and, in one case, could not get an MRI without the maker's input. Sources: IEEE Spectrum: Their bionic eyes are now obsolete and unsupported

MITIGATION PRINCIPLE

Support for an implant is planned for the life of the patient's device, including what happens if the manufacturer cannot provide it.

DESIGN MEASURES

1. Publish an end-of-support date and a support plan covering programmers, updates and vulnerability handling.
2. Escrow programmer software, keys and specifications so a successor or regulator can support patients.
3. Design implants to keep safe default therapy if their programmers and services disappear.
4. Tell patients and clinicians early when support is ending, with options.

MAPPINGS

STRIDE	D Denial of service
CAPEC	CAPEC-682 Exploitation of Firmware or ROM Code with Unpatchable Vulnerabilities
CWE	CWE-1277 Firmware Not Updateable CWE-1329 Reliance on Component That is Not Updateable
EMB3D	TID-210 Device Vulnerabilities Unpatchable
MDS2	RDMP Roadmap for third-party components, CSUP Cybersecurity product upgrades
Standards	AAMI SW96 FDA premarket IEC 81001-5-1

CRI-IM-7 Battery drained by wake-ups

† DIRECT HARM · THE PATIENT · RANK 7

THREAT

The implant's radio can be woken by unauthenticated requests. Repeated wake-ups drain a battery that cannot be recharged, forcing early replacement surgery and, before that, possible loss of therapy.

MITIGATION PROMPTS (ON THE CARD)

1. Can an unauthenticated request wake the implant's radio?
2. How much battery could repeated wake-ups cost over a month?
3. Would the clinic notice unusual radio activity draining the battery?

MITIGATION PRINCIPLE

Unauthenticated traffic cannot make the implant spend meaningful energy.

DESIGN MEASURES

1. Keep the radio asleep until a close-range, low-energy wake mechanism or a scheduled window.
2. Rate-limit wake-ups and authentication attempts, and back off sharply after failures.
3. Track energy spent on communication and raise an alert at follow-up if it is abnormal.

MAPPINGS

STRIDE	D Denial of service
CAPEC	CAPEC-125 Flooding
CWE	CWE-770 Allocation of Resources Without Limits or Throttling CWE-799 Improper Control of Interaction Frequency
ATT&CK	T1499 Endpoint Denial of Service
EMB3D	TID-405 Network Stack Resource Exhaustion
MDS2	CONN Connectivity capabilities, NAUT Node authentication
Standards	FDA premarket

CRI-IM-6 Silent remote follow-up

† CARE DELAYED OR WRONG THE PATIENT · RANK 6

THREAT

The home transmitter stops sending, is unplugged, loses its connection or sends stale data, and the clinic treats no news as good news. Alerts for arrhythmias, lead faults or low battery are missed for weeks.

MITIGATION PROMPTS (ON THE CARD)

1. How does the clinic learn that a transmitter has gone silent?
2. Who is told when follow-up data stops or goes stale?
3. Does no news get treated as good news anywhere in this process?

MITIGATION PRINCIPLE

Loss of remote follow-up is itself an alert, raised to the clinic and the patient.

DESIGN MEASURES

1. Expect a heartbeat from every transmitter and alert the clinic when one is overdue.
2. Timestamp and sequence readings so stale or repeated data is visible.
3. Tell the patient on the transmitter or their phone when it cannot reach the service.

MAPPINGS

STRIDE	D Denial of service, T Tampering
CWE	CWE-754 Improper Check for Unusual or Exceptional Conditions
ATT&CK	T0829 Loss of View
MDS2	CONN Connectivity capabilities, IGAU Health data integrity and authenticity
Standards	IEC 80001-1 ISO 14971

CRI-IM-5 Clinic programmer as the weak link

† DIRECT HARM THE PATIENT · RANK 5

THREAT

Clinic programmers run old operating systems, use shared logins and leave the building with field staff. They hold keys and patient data, and a stolen or compromised programmer can reprogram any implant of that make.

MITIGATION PROMPTS (ON THE CARD)

1. What secrets does a clinic programmer hold, and could one unlock every implant?
2. Who may use the programmer, and how is each use attributed?
3. What happens when a programmer is lost or stolen?

MITIGATION PRINCIPLE

A programmer holds no secret that unlocks every implant, and its use is tied to a named, authorised clinician.

DESIGN MEASURES

1. Use per-device or per-session keys issued by a back end, not a fixed key shared by every programmer.
2. Require clinician login on the programmer and revoke lost or stolen programmers remotely.
3. Harden and patch the programmer's operating system, and encrypt patient data stored on it.

MAPPINGS

STRIDE	S Spoofing, I Information disclosure, E Elevation of privilege
LINDDUN	DD Data disclosure
CAPEC	CAPEC-191 Read Sensitive Constants Within an Executable
CWE	CWE-321 Use of Hard-coded Cryptographic Key CWE-1104 Use of Unmaintained Third Party Components
ATT&CK	T1005 Data from Local System
EMB3D	TID-214 Secrets Extracted from Device Root of Trust
MDS2	PAUT Person authentication, PLOK Physical locks, SAHD System and application hardening
Standards	AAMI SW96 IEC 81001-5-1

CRI-IM-4 Telemetry reveals the patient

THE PATIENT · RANK 4

THREAT

Implant telemetry and home transmitter traffic travel unencrypted. Anyone nearby with a receiver learns the device serial, the patient's identity or diagnosis and their heart data.

MITIGATION PROMPTS (ON THE CARD)

1. What can a listener learn from implant or transmitter traffic?
2. Is the patient's identity or diagnosis visible on the radio link?
3. Which links between implant, transmitter and cloud are encrypted?

SEEN IN PUBLIC

Medtronic Conexus telemetry, 2019. US government advisories warned that the Conexus radio protocol used by Medtronic implantable defibrillators, clinic programmers and home monitors had no authentication or encryption, so someone nearby could read or change device settings. Sources: CISA: ICS Medical Advisory ICSMA-19-080-01

MITIGATION PRINCIPLE

Implant and transmitter traffic reveals nothing about the patient to a listener.

DESIGN MEASURES

1. Encrypt all telemetry carrying patient or device identifiers.
2. Avoid sending names or diagnoses over the radio; use identifiers the clinic resolves.
3. Verify encryption on the air during security testing, not only in the design.

MAPPINGS

STRIDE	I Information disclosure
LINDDUN	I Identifying, DD Data disclosure, L Linking
CAPEC	CAPEC-157 Sniffing Attacks
CWE	CWE-319 Cleartext Transmission of Sensitive Information
ATT&CK	T1040 Network Sniffing
EMB3D	TID-408 Unencrypted Sensitive Data Communication
MDS2	TXCF Transmission confidentiality
Standards	FDA premarket

CRI-IM-3 Radio identifiers track the patient

THE PATIENT · RANK 3

THREAT

The implant or its transmitter broadcasts a fixed identifier. It can be used to detect that a person carries a cardiac or neurological implant and to follow them between places.

MITIGATION PROMPTS (ON THE CARD)

1. Does the implant or transmitter broadcast a fixed identifier?
2. Could a stranger tell that someone carries an implant?
3. How would you stop the radio being used to follow a patient?

MITIGATION PRINCIPLE

The radio does not let a stranger recognise or follow the patient.

DESIGN MEASURES

1. Advertise only when a session is wanted, and with rotating identifiers.
2. Keep fixed serial numbers inside the encrypted session.
3. Review radio behaviour against tracking during privacy impact assessment.

MAPPINGS

STRIDE	I Information disclosure
LINDDUN	L Linking, I Identifying, D Detecting
CAPEC	CAPEC-651 Eavesdropping
CWE	CWE-359 Exposure of Private Personal Information to an Unauthorized Actor
MDS2	CONN Connectivity capabilities, TXCF Transmission confidentiality

CRI-IM-2 No route for researchers' findings

THE PATIENT · RANK 2

THREAT

Researchers and patients who find flaws in an implant have no clear way to report them, so issues stay unfixed, reach the public without a fix, or are sold. Clinicians learn about them from the news.

MITIGATION PROMPTS (ON THE CARD)

1. How does a researcher or patient report a flaw in this implant?
2. Who tells clinicians and patients what to do about a reported flaw?
3. How long does a reported implant flaw usually take to fix?

MITIGATION PRINCIPLE

The manufacturer runs coordinated vulnerability disclosure and tells clinicians and patients what to do.

DESIGN MEASURES

1. Publish a vulnerability disclosure policy and a monitored contact, and acknowledge reports promptly.
2. Agree timelines for fixes and advisories with regulators and reporters.
3. Send clinicians clear guidance on clinical risk and actions when an advisory is issued.

MAPPINGS

STRIDE	R Repudiation, I Information disclosure
CAPEC	CAPEC-188 Reverse Engineering
MDS2	SGUD Security guidance, CSUP Cybersecurity product upgrades
Standards	AAMI SW96 FDA premarket

CRI-BW · THE PATIENT · 13 ENTRIES

Body-worn and Home-use Devices

Insulin pumps, CGMs and closed loops, patch and Holter ECG, pulse oximeters, BP cuffs, hearing aids and connected inhalers, and the phones that control them.

https://ostering.com/taxonomies/hospitals-and-medical-devices/body-worn-and-home-use-devices/

CRI-BW-A Spoofed controller doses insulin

† DIRECT HARM THE PATIENT · RANK A

THREAT

The insulin pump accepts bolus and basal commands from a remote or phone app without strong pairing or authentication. A nearby attacker or rogue app can deliver a fatal overdose or quietly stop insulin.

MITIGATION PROMPTS (ON THE CARD)

1. Which controllers can send dose commands to the pump?
2. What dose limits does the pump enforce on its own?
3. How is a new controller paired, and who must confirm it?

SEEN IN PUBLIC

Medtronic MiniMed insulin pumps, 2019. The FDA warned that certain older Medtronic MiniMed insulin pumps could be reached over their radio link by someone nearby and their settings changed; Medtronic recalled them and offered replacements, as the pumps could not be updated. Sources: Infosecurity: Insulin pumps recalled by FDA for cybersecurity risks; Becker's: Medtronic recalls insulin pumps that can be wirelessly hacked

MITIGATION PRINCIPLE

A pump acts only on dose commands from a paired, authenticated controller, within limits it enforces itself.

DESIGN MEASURES

1. Require authenticated, encrypted pairing and verify every dose command's origin and integrity.
2. Enforce maximum bolus and daily limits in the pump, whatever the controller asks.
3. Ask for confirmation on the pump or the paired phone before large boluses.
4. Alert the user on the pump when an unknown device tries to connect.

MAPPINGS

STRIDE	S Spoofing, T Tampering, E Elevation of privilege
CAPEC	CAPEC-151 Identity Spoofing CAPEC-594 Traffic Injection
CWE	CWE-306 Missing Authentication for Critical Functionality CWE-290 Authentication Bypass by Spoofing
ATT&CK	T0831 Manipulation of Control
EMB3D	TID-406 Unauthorized Messages or Connections
MDS2	NAUT Node authentication, AUTH Authorization, TXIG Transmission integrity
Standards	FDA premarket AAMI SW96

CRI-BW-K Closed loop trusts a spoofed sensor

† DIRECT HARM THE PATIENT · RANK K

THREAT

An automated insulin delivery algorithm doses from glucose sensor readings with no person in the loop. A spoofed, replayed or faulty reading drives it to overdose or withhold insulin, overnight, while the patient sleeps.

MITIGATION PROMPTS (ON THE CARD)

1. How does the dosing algorithm know a sensor reading is genuine?
2. What does the loop do when readings look implausible?
3. What bounds stop the loop overdosing while the patient sleeps?

MITIGATION PRINCIPLE

Automated dosing trusts only authenticated sensor data and stays within safe bounds when data looks wrong.

DESIGN MEASURES

1. Authenticate the sensor to the controller and protect readings against injection and replay.
2. Check readings for physiological plausibility and rate of change before dosing on them.
3. Fall back to a conservative basal rate and alert when sensor data is missing or implausible.

MAPPINGS

STRIDE	S Spoofing, T Tampering
CAPEC	CAPEC-194 Fake the Source of Data
CWE	CWE-1293 Missing Source Correlation of Multiple Independent Data CWE-940 Improper Verification of Source of a Communication Channel
ATT&CK	T1565.002 Transmitted Data Manipulation
EMB3D	TID-406 Unauthorized Messages or Connections
MDS2	NAUT Node authentication, IGAU Health data integrity and authenticity
Standards	FDA premarket ISO 14971

CRI-BW-Q Phone app as the controller

† DIRECT HARM THE PATIENT · RANK Q

THREAT

The app that controls a pump or reads a sensor runs on a phone the manufacturer does not control: rooted, out of date, shared, full of other apps. Malware or an operating system change can alter doses or stop the app working.

MITIGATION PROMPTS (ON THE CARD)

1. Which safety decisions are made on the phone rather than the device?
2. What happens to therapy if the phone is rooted or out of date?
3. How does the app behave after an operating system update?

MITIGATION PRINCIPLE

A therapy-critical app assumes the phone may be hostile and keeps safety decisions on the medical device.

DESIGN MEASURES

1. Keep dose limits and safety checks on the pump, never only in the app.
2. Check the phone's integrity and operating system version, and warn or degrade safely when unsupported.
3. Publish a list of supported phones and versions, and test new operating system releases before users get them.

MAPPINGS

STRIDE	T Tampering, E Elevation of privilege, D Denial of service
CAPEC	CAPEC-441 Malicious Logic Insertion
CWE	CWE-1357 Reliance on Insufficiently Trustworthy Component CWE-602 Client-Side Enforcement of Server-Side Security
MDS2	MLDP Malware detection and protection, RDMP Roadmap for third-party components, SGUD Security guidance
Standards	IEC 81001-5-1 IEC 62304

CRI-BW-J Firmware pushed through the phone

† DIRECT HARM THE PATIENT · RANK J

THREAT

Device updates arrive through the companion app without the device verifying them, or install at a bad moment. A modified update takes control of therapy, and a failed one leaves the patient without insulin or monitoring at night.

MITIGATION PROMPTS (ON THE CARD)

1. Does the device verify an update itself, or trust the app?
2. When is an update allowed to install, and who decides?
3. What does the patient do if an update fails overnight?

MITIGATION PRINCIPLE

The device verifies every update itself and installs only when therapy can safely pause or continue.

DESIGN MEASURES

1. Verify a manufacturer signature on the device; never rely on the app to check.
2. Schedule installation with the user and keep therapy running from the previous image until the new one is proven.
3. Prevent rollback to vulnerable versions and keep a recovery image.

MAPPINGS

STRIDE	T Tampering, D Denial of service, E Elevation of privilege
CAPEC	CAPEC-186 Malicious Software Update
CWE	CWE-494 Download of Code Without Integrity Check CWE-347 Improper Verification of Cryptographic Signature
ATT&CK	T1495 Firmware Corruption
EMB3D	TID-211 Device Allows Unauthenticated Firmware Installation TID-217 Remotely Initiated Updates Can Cause DoS
MDS2	CSUP Cybersecurity product upgrades, IGAU Health data integrity and authenticity
Standards	FDA premarket

CRI-BW-10 Cloud account takeover

† DIRECT HARM THE PATIENT · RANK 10

THREAT

Manufacturer cloud accounts for patients and caregivers use reused passwords and no second factor. Taking one over exposes years of readings and, where the service allows, changes alarm thresholds or therapy settings remotely.

MITIGATION PROMPTS (ON THE CARD)

1. What can a caregiver or patient cloud account change remotely?
2. Do cloud accounts need a second factor before changing settings?
3. Who is alerted when alarm thresholds change from the cloud?

MITIGATION PRINCIPLE

Cloud accounts that can see or change therapy are protected like clinical systems.

DESIGN MEASURES

1. Offer and encourage multi-factor authentication, and require it for any account that can change settings.
2. Detect credential stuffing and unusual logins, and notify the patient of new devices.
3. Require confirmation on the medical device for any remote settings change.

MAPPINGS

STRIDE	S Spoofing, I Information disclosure, T Tampering
LINDDUN	I Identifying, DD Data disclosure
CAPEC	CAPEC-600 Credential Stuffing
CWE	CWE-308 Use of Single-factor Authentication CWE-307 Improper Restriction of Excessive Authentication Attempts
ATT&CK	T1078 Valid Accounts T1110 Brute Force
MDS2	PAUT Person authentication, AUTH Authorization
Standards	IEC 81001-5-1

CRI-BW-9 Alarms lost on the phone

† CARE DELAYED OR WRONG THE PATIENT · RANK 9

THREAT

Low and high glucose or arrhythmia alerts travel through the phone. Battery optimisation, do-not-disturb, revoked permissions or an operating system update silence them, and nobody notices the alarm path has broken until a patient is harmed.

MITIGATION PROMPTS (ON THE CARD)

1. What on the phone could silence a low glucose alert?
2. How would anyone know the alarm path had broken?
3. Is there a second route for critical alerts besides the phone?

MITIGATION PRINCIPLE

The alarm path is monitored end to end, and a broken path is itself loud.

DESIGN MEASURES

1. Use critical-alert channels where the platform offers them, and check permissions on every launch.
2. Send a periodic test or heartbeat and warn the user when the app cannot raise alerts.
3. Keep an audible alarm on the medical device itself for the most dangerous conditions.

MAPPINGS

STRIDE	D Denial of service
CWE	CWE-754 Improper Check for Unusual or Exceptional Conditions
ATT&CK	T0878 Alarm Suppression
MDS2	SGUD Security guidance, CONN Connectivity capabilities
Standards	IEC 80001-1 ISO 14971

CRI-BW-8 Radio stack crash stops therapy

† DIRECT HARM THE PATIENT · RANK 8

THREAT

Malformed Bluetooth packets crash or hang the device's radio chip or stack. Readings stop, the pump or hearing aid freezes, and the device may not restart into a safe state until someone notices.

MITIGATION PROMPTS (ON THE CARD)

1. What happens to therapy if the radio stack crashes or hangs?
2. Does the device restart into a safe state on its own?
3. Has the Bluetooth stack been tested against malformed packets?

SEEN IN PUBLIC

SweynTooth Bluetooth flaws, 2020. The FDA warned that SweynTooth flaws in Bluetooth Low Energy chips used in pacemakers, glucose monitors, insulin pumps and other devices could let someone nearby crash a device, stop it working or bypass security. Sources: RAPS: FDA warns of cybersecurity vulnerabilities in pacemakers and other BLE devices; HPN: FDA informs about potential vulnerabilities in medical devices with Bluetooth Low Energy

MITIGATION PRINCIPLE

Faults in the radio stack cannot stop therapy or leave the device in an unsafe state.

DESIGN MEASURES

1. Isolate the radio from therapy logic so a radio fault cannot halt delivery or sensing.
2. Use a watchdog that restarts the radio and alerts the user without interrupting therapy.
3. Track vulnerabilities in the radio chip's software and fuzz the stack before release.

MAPPINGS

STRIDE	D Denial of service
CAPEC	CAPEC-666 BlueSmacking CAPEC-28 Fuzzing
CWE	CWE-617 Reachable Assertion CWE-754 Improper Check for Unusual or Exceptional Conditions
ATT&CK	T1499 Endpoint Denial of Service
EMB3D	TID-202 Exploitable System Network Stack Component TID-404 Remotely Triggerable Deadlock/DoS
MDS2	SAHD System and application hardening, CSUP Cybersecurity product upgrades
Standards	FDA premarket

CRI-BW-7 Weak pairing invites strangers

† DIRECT HARM THE PATIENT · RANK 7

THREAT

Pairing uses fixed PINs, legacy modes or no confirmation, or lets a nearby device push the link down to weak encryption. A stranger pairs, listens in or injects readings and commands.

MITIGATION PROMPTS (ON THE CARD)

1. How does pairing confirm the user really meant to pair?
2. Can a nearby device force the link down to weaker encryption?
3. Which pairing modes remain enabled that nobody needs?

SEEN IN PUBLIC

SweynTooth Bluetooth flaws, 2020. The FDA warned that SweynTooth flaws in Bluetooth Low Energy chips used in pacemakers, glucose monitors, insulin pumps and other devices could let someone nearby crash a device, stop it working or bypass security. Sources: RAPS: FDA warns of cybersecurity vulnerabilities in pacemakers and other BLE devices; HPN: FDA informs about potential vulnerabilities in medical devices with Bluetooth Low Energy

MITIGATION PRINCIPLE

Pairing is deliberate, confirmed by the user and resistant to downgrade.

DESIGN MEASURES

1. Use authenticated pairing with out-of-band confirmation such as a code shown on the device.
2. Refuse legacy pairing and keys shorter than current standards allow.
3. Show paired devices to the user and let them remove any they do not recognise.

MAPPINGS

STRIDE	S Spoofing, I Information disclosure, T Tampering
LINDDUN	DD Data disclosure
CAPEC	CAPEC-668 Key Negotiation of Bluetooth Attack (KNOB) CAPEC-667 Bluetooth Impersonation AttackS (BIAS) CAPEC-620 Drop Encryption Level
CWE	CWE-1390 Weak Authentication CWE-326 Inadequate Encryption Strength
ATT&CK	T0860 Wireless Compromise
EMB3D	TID-411 Weak/Insecure Cryptographic Protocol
MDS2	NAUT Node authentication, TXCF Transmission confidentiality
Standards	FDA premarket

CRI-BW-6 No supported way to automate

† DIRECT HARM THE PATIENT · RANK 6

THREAT

With no supported way to automate their therapy, some patients build or download unofficial loops that drive older pumps through weak radio protocols. Nobody else knows what is dosing, and vulnerable pumps stay in service by choice.

MITIGATION PROMPTS (ON THE CARD)

1. Do patients have a supported way to automate their therapy?
2. Would the device or clinic notice an unofficial controller dosing?
3. Which older pumps stay in service because unofficial loops need them?

MITIGATION PRINCIPLE

Patients have a supported, secure way to get the automation they need, and devices make unofficial control visible.

DESIGN MEASURES

1. Offer supported interoperability through authenticated, documented interfaces.
2. Record on the device which controller issued each dose so clinicians can see it.
3. Give clinicians guidance on reviewing patients who use unofficial controllers, without penalising them.

MAPPINGS

STRIDE	S Spoofing, R Repudiation, E Elevation of privilege
CAPEC	CAPEC-212 Functionality Misuse
CWE	CWE-1357 Reliance on Insufficiently Trustworthy Component
MDS2	RDMP Roadmap for third-party components, CONN Connectivity capabilities, AUDT Audit controls
Standards	IEC 80001-1

CRI-BW-5 Home readings without provenance

† CARE DELAYED OR WRONG · THE PATIENT · RANK 5

THREAT

Readings from home blood pressure cuffs, pulse oximeters or ECG patches upload with no way to tell which device or person produced them. A family member's, replayed or edited values enter the record and shape treatment.

MITIGATION PROMPTS (ON THE CARD)

1. How does the record know which device and patient produced a reading?
2. Could a family member's or replayed reading enter the record?
3. Which home readings change treatment without a clinician checking them?

MITIGATION PRINCIPLE

Every home reading carries authenticated provenance: which device, which patient, when.

DESIGN MEASURES

1. Bind each device to one patient at enrolment and sign readings on the device.
2. Show provenance and any manual edits beside the reading in the clinical record.
3. Flag readings that arrive late, out of sequence or from an unbound device.

MAPPINGS

STRIDE	S Spoofing, T Tampering, R Repudiation
LINDDUN	I Identifying
CAPEC	CAPEC-194 Fake the Source of Data
CWE	CWE-346 Origin Validation Error CWE-1293 Missing Source Correlation of Multiple Independent Data
ATT&CK	T1565.002 Transmitted Data Manipulation
EMB3D	TID-406 Unauthorized Messages or Connections
MDS2	IGAU Health data integrity and authenticity, NAUT Node authentication
Standards	IEC 81001-5-1

CRI-BW-4 Own devices on the ward

† CARE DELAYED OR WRONG · THE PATIENT · RANK 4

THREAT

Patients bring their own pumps, sensors, hearing aids and phones into hospital. Staff cannot read or control them, they join the guest network or lose their cloud link, and nobody owns their security or the clinical decisions they drive.

MITIGATION PROMPTS (ON THE CARD)

1. What is the process for accepting a patient's own device on the ward?
2. Who owns the security of patients' own devices while they are inpatients?
3. Which network do patients' devices join, and what can they reach?

MITIGATION PRINCIPLE

The hospital has an agreed way to accept, use and support patients' own devices.

DESIGN MEASURES

1. Define a policy for patients' own devices covering who reviews them and how therapy is handed over.
2. Provide a network path for them that keeps their cloud link without reaching clinical systems.
3. Record in the patient's notes which personal devices are in use and their settings.

MAPPINGS

STRIDE	D Denial of service, T Tampering
CAPEC	CAPEC-700 Network Boundary Bridging
CWE	CWE-1357 Reliance on Insufficiently Trustworthy Component
MDS2	CONN Connectivity capabilities, SGUD Security guidance
Standards	IEC 80001-1

CRI-BW-3 Companion apps sell health data

THE PATIENT · RANK 3

THREAT

Companion apps for inhalers, sensors and monitors carry analytics and advertising code that sends device identifiers and readings to third parties. Patients do not know, and the data links them to a condition for years.

MITIGATION PROMPTS (ON THE CARD)

1. Which third parties receive data from the companion app?
2. Does the patient know what leaves the app, and agree to it?
3. What analytics or advertising code ships inside the app?

MITIGATION PRINCIPLE

Health data leaves the app only for the patient's care, and only with their informed agreement.

DESIGN MEASURES

1. Inventory every third-party SDK in the app and remove any that receive health or device data.
2. Collect the minimum data and state each use in plain language before collection.
3. Let patients see, export and delete what is held about them.

MAPPINGS

STRIDE	I Information disclosure
LINDDUN	L Linking, I Identifying, U Unawareness and unintervenability, DD Data disclosure, Nc Non-compliance
CAPEC	CAPEC-569 Collect Data as Provided by Users
CWE	CWE-359 Exposure of Private Personal Information to an Unauthorized Actor
MDS2	MPII Management of private data, DIDT Health data de-identification
Standards	ISO 27799

CRI-BW-2 Second-hand devices keep old data

THE PATIENT · RANK 2

THREAT

Devices that are resold, loaned, refurbished or reused across family phones keep the previous patient's data, pairings or cloud account link. The new user's readings flow to someone else's account or clinic.

MITIGATION PROMPTS (ON THE CARD)

1. What is wiped when a device changes user or is refurbished?
2. Which pairings and cloud links survive a change of owner?
3. How would a new user notice data flowing to someone else?

MITIGATION PRINCIPLE

Every change of user wipes the device and breaks every old link.

DESIGN MEASURES

1. Provide a factory reset that erases data, pairings and account links, and verify it.
2. Require fresh enrolment with the clinic before a reused device sends readings.
3. Tell patients how to reset devices before passing them on.

MAPPINGS

STRIDE	I Information disclosure
LINDDUN	DD Data disclosure, L Linking, I Identifying
CAPEC	CAPEC-675 Retrieve Data from Decommissioned Devices
CWE	CWE-1266 Improper Scrubbing of Sensitive Data from Decommissioned Device CWE-226 Sensitive Information in Resource Not Removed Before Reuse
MDS2	MPII Management of private data, STCF Data storage confidentiality

CRI-PM · THE PATIENT · 13 ENTRIES

Patient Monitoring

Bedside monitors (ECG, SpO2, NIBP and invasive BP, heart rate, respiration, capnography, temperature), central stations, telemetry and early-warning feeds.

https://ostering.com/taxonomies/hospitals-and-medical-devices/patient-monitoring/

CRI-PM-A False values on the monitor

† CARE DELAYED OR WRONG THE PATIENT · RANK A

THREAT

Monitors and central stations accept data from the monitoring network without checking its source or integrity. Altered values show normal SpO2, heart rate and blood pressure while the patient deteriorates, or alarming values for a stable one, and staff treat the screen.

MITIGATION PROMPTS (ON THE CARD)

1. How does the central station know data came from a genuine monitor?
2. What protects vital signs in transit across the monitoring network?
3. Would staff notice values that look normal but are false?

SEEN IN PUBLIC

MDhex, GE patient monitoring, 2020. CISA published six vulnerabilities (MDhex) in GE Healthcare CARESCAPE telemetry servers, central stations and related patient monitoring products, including hard-coded credentials, that could let an attacker change alarm settings or make devices unusable. Sources: Help Net Security: MDhex vulnerabilities open GE patient monitoring devices to attackers; Computer Weekly: NHS alerted to severe vulnerabilities in GE health equipment

MITIGATION PRINCIPLE

Displayed vital signs come only from authenticated devices over integrity-protected links.

DESIGN MEASURES

1. Authenticate monitors to central stations and gateways, and protect each message for integrity.
2. Show the source device and data age beside every value at the central station.
3. Cross-check related signals, such as SpO2 pulse rate against ECG heart rate, and flag disagreement.

MAPPINGS

STRIDE	S Spoofing, T Tampering
CAPEC	CAPEC-194 Fake the Source of Data CAPEC-148 Content Spoofing
CWE	CWE-924 Improper Enforcement of Message Integrity During Transmission in a Communication Channel CWE-306 Missing Authentication for Critical Functionality
ATT&CK	T0832 Manipulation of View T1565.002 Transmitted Data Manipulation
EMB3D	TID-406 Unauthorized Messages or Connections
MDS2	TXIG Transmission integrity, NAUT Node authentication
Standards	IEC TR 60601-4-5 FDA premarket

CRI-PM-K Alarms silenced from afar

† CARE DELAYED OR WRONG THE PATIENT · RANK K

THREAT

Alarm limits, volume and pause states can be changed from a central station, a remote viewer or the network without authorisation, and alarm forwarding can be turned off. Deterioration alarms never reach a nurse.

MITIGATION PROMPTS (ON THE CARD)

1. Who can change alarm limits, and from where?
2. Does the bedside show a remote change, and who made it?
3. Can anyone turn alarm forwarding off without a clinician knowing?

MITIGATION PRINCIPLE

Changes to alarm behaviour are authorised, local where possible, visible and logged.

DESIGN MEASURES

1. Require clinician authentication for changes to alarm limits, volume or forwarding.
2. Show any non-default alarm setting prominently on the bedside monitor.
3. Log every alarm configuration change with who made it and from where.
4. Prevent alarms being turned off entirely from remote stations.

MAPPINGS

STRIDE	T Tampering, E Elevation of privilege, R Repudiation
CAPEC	CAPEC-176 Configuration/Environment Manipulation
CWE	CWE-862 Missing Authorization CWE-306 Missing Authentication for Critical Functionality
ATT&CK	T0838 Modify Alarm Settings T0878 Alarm Suppression
EMB3D	TID-310 Remotely Accessible Unauthenticated Services
MDS2	AUTH Authorization, AUDT Audit controls
Standards	IEC TR 60601-4-5 ISO 14971

CRI-PM-Q Telemetry dropout looks quiet

† CARE DELAYED OR WRONG THE PATIENT · RANK Q

THREAT

Wireless telemetry is jammed or drops out and the central station keeps showing the last value or no alarm, instead of a loud loss-of-signal. A patient walking off the ward or behind a lift shaft goes unmonitored.

MITIGATION PROMPTS (ON THE CARD)

1. What does the central station show when telemetry drops out?
2. Where on the ward does telemetry coverage fail?
3. Is loss of signal an alarm, or just a blank tile?

MITIGATION PRINCIPLE

Loss of monitoring is treated as an alarm in its own right.

DESIGN MEASURES

1. Raise a technical alarm as soon as telemetry is lost, with escalation if it persists.
2. Mark stale values clearly and never show them as current.
3. Survey wireless coverage and monitor the band for interference and jamming.

MAPPINGS

STRIDE	D Denial of service
CAPEC	CAPEC-601 Jamming CAPEC-604 Wi-Fi Jamming
CWE	CWE-754 Improper Check for Unusual or Exceptional Conditions CWE-636 Not Failing Securely
ATT&CK	T0815 Denial of View T0829 Loss of View
MDS2	CONN Connectivity capabilities
Standards	IEC 80001-1 IEC TR 60601-4-5

CRI-PM-J Wrong patient on the monitor

† CARE DELAYED OR WRONG THE PATIENT · RANK J

THREAT

The link between monitor, bed and patient admission is wrong or can be changed without checks. Readings and alarms are charted to another patient, sent to the wrong nurse, and drive someone else's treatment.

MITIGATION PROMPTS (ON THE CARD)

1. How is a monitor linked to the right patient and bed?
2. Who can change that link, and is the change checked?
3. Where can staff see which patient a monitor belongs to?

MITIGATION PRINCIPLE

Every monitor-to-patient association is verified when made and visible all the time.

DESIGN MEASURES

1. Confirm association by scanning the patient's wristband at the monitor.
2. Show the patient's name and identifier on the monitor and at the central station.
3. Log association changes and alert when a monitor is reassigned while readings are flowing.

MAPPINGS

STRIDE	S Spoofing, T Tampering
LINDDUN	DD Data disclosure
CAPEC	CAPEC-151 Identity Spoofing
CWE	CWE-1293 Missing Source Correlation of Multiple Independent Data
ATT&CK	T1565.001 Stored Data Manipulation
MDS2	IGAU Health data integrity and authenticity, AUDT Audit controls
Standards	IEC 80001-1

CRI-PM-10 Early-warning score goes stale

† CARE DELAYED OR WRONG THE PATIENT · RANK 10

THREAT

Vital signs feed early-warning and sepsis scores in the record. If the feed stops or lags, the score keeps its last value and no escalation is triggered, while staff believe the system is watching.

MITIGATION PROMPTS (ON THE CARD)

1. How fresh are the inputs behind the early-warning score?
2. What alerts staff when the vital signs feed stops?
3. Would a stale score look any different from a current one?

MITIGATION PRINCIPLE

A score shows how fresh its inputs are and alerts when they are not.

DESIGN MEASURES

1. Timestamp every input and show its age with the score.
2. Alert when expected observations are overdue for a patient.
3. Monitor the interface feeding the score and page someone when it stops.

MAPPINGS

STRIDE	D Denial of service, T Tampering
CWE	CWE-754 Improper Check for Unusual or Exceptional Conditions CWE-1088 Synchronous Access of Remote Resource without Timeout
ATT&CK	T0829 Loss of View
MDS2	IGAU Health data integrity and authenticity, CONN Connectivity capabilities
Standards	IEC 80001-1

CRI-PM-9 Monitors as network footholds

† CARE DELAYED OR WRONG THE PATIENT · RANK 9

THREAT

Monitors and central stations run old embedded or desktop operating systems with exposed services that cannot be patched quickly. One compromised device becomes a route to other monitors and the clinical network.

MITIGATION PROMPTS (ON THE CARD)

1. Which services do monitors and central stations expose on the network?
2. How quickly can a monitor vulnerability actually be patched?
3. What else could a compromised monitor reach?

SEEN IN PUBLIC

MDhex, GE patient monitoring, 2020. CISA published six vulnerabilities (MDhex) in GE Healthcare CARESCAPE telemetry servers, central stations and related patient monitoring products, including hard-coded credentials, that could let an attacker change alarm settings or make devices unusable. Sources: Help Net Security: MDhex vulnerabilities open GE patient monitoring devices to attackers; Computer Weekly: NHS alerted to severe vulnerabilities in GE health equipment

URGENT/11, 2019. The FDA warned that 11 vulnerabilities in IPnet, a third-party network stack inside several embedded operating systems, could let attackers take over or crash medical devices and hospital network equipment, and that manufacturers might not know their products contained it. Sources: Healthcare IT News: URGENT/11, FDA issues alert

MITIGATION PRINCIPLE

Monitoring devices expose only what they need and sit where a compromise cannot spread.

DESIGN MEASURES

1. Disable unused services and ports, and document the rest for the hospital.
2. Place monitors in their own network segment with traffic only to their central station and gateway.
3. Publish patch and support timelines and validate security fixes quickly.
4. Supply an SBOM so the hospital can track vulnerable components.

MAPPINGS

STRIDE	E Elevation of privilege, D Denial of service, T Tampering
CAPEC	CAPEC-682 Exploitation of Firmware or ROM Code with Unpatchable Vulnerabilities
CWE	CWE-1104 Use of Unmaintained Third Party Components CWE-1395 Dependency on Vulnerable Third-Party Component
ATT&CK	T0866 Exploitation of Remote Services T1210 Exploitation of Remote Services
EMB3D	TID-202 Exploitable System Network Stack Component TID-210 Device Vulnerabilities Unpatchable
MDS2	SAHD System and application hardening, CSUP Cybersecurity product upgrades, SBOM Software bill of materials
Standards	IEC 80001-1 IEC 81001-5-1

CRI-PM-8 Monitor firmware phones home

† CARE DELAYED OR WRONG THE PATIENT · RANK 8

THREAT

Monitor firmware contains hidden functions that send patient data to fixed external addresses or fetch and run files from them. Nobody at the hospital knows the function exists until it is reported.

MITIGATION PROMPTS (ON THE CARD)

1. Which external addresses do the monitors contact?
2. Who configured each destination a monitor connects to?
3. How would the hospital discover hidden functions in monitor firmware?

SEEN IN PUBLIC

Contec CMS8000 patient monitors, 2025. CISA and the FDA warned that Contec CMS8000 patient monitors made hidden connections to a hard-coded internet address, could download and run unverified files, and sent patient data in plain text when a patient was connected; with no fix available, CISA advised unplugging them. A researcher later argued it was more likely insecure design than deliberate backdoor. Sources: CISA: Fact sheet, Contec CMS8000 contains a backdoor; The Hacker News: CISA and FDA warn of critical backdoor in Contec CMS8000

MITIGATION PRINCIPLE

A monitor connects only to destinations the hospital configured, and contains no hidden functionality.

DESIGN MEASURES

1. Review firmware and third-party components for undeclared network functions before purchase and release.
2. Let the hospital configure, and see, every outbound destination.
3. Block monitor traffic to the internet by default at the network edge.

MAPPINGS

STRIDE	I Information disclosure, E Elevation of privilege
LINDDUN	DD Data disclosure, U Unawareness and unintervenability
CAPEC	CAPEC-443 Malicious Logic Inserted Into Product by Authorized Developer
CWE	CWE-912 Hidden Functionality CWE-506 Embedded Malicious Code
ATT&CK	T0862 Supply Chain Compromise
EMB3D	TID-401 Undocumented Protocol Features
MDS2	CONN Connectivity capabilities, SBOM Software bill of materials
Standards	FDA premarket IEC 81001-5-1

CRI-PM-7 Service menus behind default passwords

† CARE DELAYED OR WRONG THE PATIENT · RANK 7

THREAT

Service and configuration menus on monitors use default or shared passwords published in manuals. Anyone with the password changes alarm defaults, calibration or network settings, and the change looks like normal behaviour.

MITIGATION PROMPTS (ON THE CARD)

1. Who knows the service password, and is it the same everywhere?
2. Is every change made through a service menu logged?
3. Could a calibration change be told apart from normal behaviour?

MITIGATION PRINCIPLE

Service access needs individual credentials and leaves a trace.

DESIGN MEASURES

1. Ship without default service passwords and require a unique one at installation.
2. Separate clinical configuration from engineering functions with different roles.
3. Log service-mode entry and every configuration change.

MAPPINGS

STRIDE	E Elevation of privilege, T Tampering, R Repudiation
CAPEC	CAPEC-70 Try Common or Default Usernames and Passwords
CWE	CWE-1392 Use of Default Credentials CWE-798 Use of Hard-coded Credentials
ATT&CK	T1078 Valid Accounts
EMB3D	TID-311 Default Credentials TID-328 Hardcoded Credentials
MDS2	PAUT Person authentication, AUTH Authorization, AUDT Audit controls
Standards	IEC TR 60601-4-5

CRI-PM-6 Clocks drift apart

† CARE DELAYED OR WRONG THE PATIENT · RANK 6

THREAT

Monitor and central station clocks are not synchronised, or their time source can be spoofed. Alarms, ECG strips, events and drug times land out of order in the record, misleading diagnosis and undermining the record as evidence.

MITIGATION PROMPTS (ON THE CARD)

1. What time source do monitors and the central station use?
2. Could that time source be spoofed or lost?
3. How would the record show that a device clock was wrong?

MITIGATION PRINCIPLE

Every device keeps trusted, synchronised time, and the record shows when it did not.

DESIGN MEASURES

1. Synchronise clocks to an authenticated hospital time source.
2. Alert when a device's clock drifts beyond a set tolerance.
3. Record both device time and receipt time for each event.

MAPPINGS

STRIDE	T Tampering, R Repudiation
CWE	CWE-1293 Missing Source Correlation of Multiple Independent Data
MDS2	AUDT Audit controls, IGAU Health data integrity and authenticity
Standards	IEC 80001-1

CRI-PM-5 Remote viewing open to the internet

† CARE DELAYED OR WRONG THE PATIENT · RANK 5

THREAT

Remote viewers let doctors watch live waveforms from home. Exposed to the internet with weak logins, they leak patients' data and, where they can silence alarms or change settings, give an outsider control.

MITIGATION PROMPTS (ON THE CARD)

1. How do doctors reach remote viewing from outside the hospital?
2. Can remote viewing silence alarms or change settings?
3. Who reviews remote viewing logins and failed attempts?

MITIGATION PRINCIPLE

Remote viewing is read-only by default and reachable only through the hospital's controlled remote access.

DESIGN MEASURES

1. Publish remote viewers only behind the hospital's remote access with multi-factor authentication.
2. Make remote viewing read-only unless a specific, logged role needs control.
3. Scan regularly for monitoring interfaces reachable from the internet.

MAPPINGS

STRIDE	I Information disclosure, E Elevation of privilege, S Spoofing
LINDDUN	DD Data disclosure, I Identifying
CAPEC	CAPEC-115 Authentication Bypass
CWE	CWE-306 Missing Authentication for Critical Functionality CWE-308 Use of Single-factor Authentication
ATT&CK	T1133 External Remote Services T1190 Exploit Public-Facing Application
EMB3D	TID-310 Remotely Accessible Unauthenticated Services
MDS2	PAUT Person authentication, RMOT Remote service, AUTH Authorization
Standards	IEC 80001-1

CRI-PM-4 Waveform archives stolen in bulk

THE PATIENT · RANK 4

THREAT

Central stations and gateways store waveforms, ECGs and alarm histories unencrypted. Theft of the store reveals cardiac diagnoses for every patient monitored in years.

MITIGATION PROMPTS (ON THE CARD)

1. Where are waveforms, ECGs and alarm histories stored, and is that encrypted?
2. How long is stored monitoring data kept?
3. Who can copy the whole monitoring archive?

MITIGATION PRINCIPLE

Stored monitoring data is encrypted and kept no longer than needed.

DESIGN MEASURES

1. Encrypt waveform and event stores at rest with keys held off the device.
2. Set retention periods and delete data once it has been written to the record.
3. Restrict export of waveform data to authorised roles and log it.

MAPPINGS

STRIDE	I Information disclosure
LINDDUN	DD Data disclosure, I Identifying
CAPEC	CAPEC-545 Pull Data from System Resources
CWE	CWE-312 Cleartext Storage of Sensitive Information
ATT&CK	T1005 Data from Local System
MDS2	STCF Data storage confidentiality, MPII Management of private data
Standards	ISO 27799

CRI-PM-3 Spot checks under a shared login

THE PATIENT · RANK 3

THREAT

Portable vital-signs devices upload observations under a generic ward login. Nobody can tell who took a reading or entered a manual value, so mistakes and falsified observations cannot be traced.

MITIGATION PROMPTS (ON THE CARD)

1. Can you tell who took each observation?
2. Which devices upload under a shared ward login?
3. How would a falsified manual value be traced?

MITIGATION PRINCIPLE

Every observation is attributed to the person who took it.

DESIGN MEASURES

1. Require badge-tap or quick login per user on spot-check devices.
2. Mark manually entered values differently from measured ones in the record.
3. Log who submitted each observation and from which device.

MAPPINGS

STRIDE	R Repudiation
LINDDUN	Nr Non-repudiation
CWE	CWE-778 Insufficient Logging
MDS2	PAUT Person authentication, AUDT Audit controls
Standards	IEC 80001-1

CRI-PM-2 Discovery traffic maps the ward

THE PATIENT · RANK 2

THREAT

Monitors announce themselves on the network with patient names, bed numbers and demographics in discovery and multicast traffic. Anyone on that network can map who is in which bed and what is being monitored.

MITIGATION PROMPTS (ON THE CARD)

1. What patient data do monitors broadcast in discovery traffic?
2. Who else shares the network segment where monitors announce themselves?
3. Could the bed board be rebuilt from network traffic alone?

MITIGATION PRINCIPLE

Network announcements carry no patient data.

DESIGN MEASURES

1. Remove patient identifiers from discovery and multicast messages.
2. Encrypt traffic that must carry patient context.
3. Keep monitor discovery traffic inside the monitoring segment.

MAPPINGS

STRIDE	I Information disclosure
LINDDUN	I Identifying, L Linking, D Detecting
CAPEC	CAPEC-292 Host Discovery
CWE	CWE-319 Cleartext Transmission of Sensitive Information CWE-359 Exposure of Private Personal Information to an Unauthorized Actor
ATT&CK	T0846 Remote System Discovery
EMB3D	TID-408 Unencrypted Sensitive Data Communication
MDS2	TXCF Transmission confidentiality, CONN Connectivity capabilities
Standards	IEC 80001-1

CRI-LS · THE PATIENT · 13 ENTRIES

Life Support and Therapy

Ventilators and respirators, anaesthesia workstations, oxygen, defibrillators, dialysis, ECMO, neonatal incubators and surgical robots.

https://ostering.com/taxonomies/hospitals-and-medical-devices/life-support-and-therapy/

CRI-LS-A Ventilation settings changed remotely

† DIRECT HARM THE PATIENT · RANK A

THREAT

The ventilator accepts changes to tidal volume, oxygen fraction, pressure or rate over the network or a connected gateway without a person at the bedside confirming them. A remote change can starve or injure a patient while the screen and the chart look normal.

MITIGATION PROMPTS (ON THE CARD)

1. Which ventilator settings can change without someone at the bedside?
2. What confirms a remote change before it reaches the patient?
3. Would the screen and chart reveal a change made remotely?

MITIGATION PRINCIPLE

Therapy-critical settings on life support change only with a local, deliberate action by a clinician at the device.

DESIGN MEASURES

1. Make network interfaces read-only for therapy parameters; any remote write path must be removed or disabled by default.
2. Require on-device confirmation, showing old and new values, for every therapy change regardless of where it originated.
3. Log every setting change with source, user and time, and alarm locally when a change arrives from outside the device.

MAPPINGS

STRIDE	T Tampering, E Elevation of privilege
CAPEC	CAPEC-137 Parameter Injection CAPEC-212 Functionality Misuse
CWE	CWE-306 Missing Authentication for Critical Functionality CWE-862 Missing Authorization
ATT&CK	T0836 Modify Parameter T0831 Manipulation of Control
EMB3D	TID-310 Remotely Accessible Unauthenticated Services TID-406 Unauthorized Messages or Connections
MDS2	AUTH Authorization, NAUT Node authentication, TXIG Transmission integrity
Standards	IEC TR 60601-4-5 ISO 14971 FDA premarket

CRI-LS-K Failure state that stops support

† DIRECT HARM THE PATIENT · RANK K

THREAT

When the ventilator, ECMO or heart-lung machine meets an unexpected message, crash or update, it reboots, stops or falls back to factory defaults instead of continuing the last safe therapy. A crafted packet or a faulty update can leave a dependent patient without support.

MITIGATION PROMPTS (ON THE CARD)

1. What does the device do after a crash, bad message or failed update?
2. Does it resume the last safe therapy or factory defaults?
3. How was the failure state tested with a patient connected?

MITIGATION PRINCIPLE

A life-support device keeps delivering its last verified therapy through software, network and update failures.

DESIGN MEASURES

1. Separate the therapy control function from networking and user interface software so a fault in one cannot stop the other.
2. Define and test a continue-last-safe-therapy state for every fault, including malformed input and failed updates.
3. Fuzz every network and data interface during verification, and treat any loss of therapy as a safety failure, not a bug.

MAPPINGS

STRIDE	D Denial of service
CAPEC	CAPEC-153 Input Data Manipulation CAPEC-125 Flooding
CWE	CWE-636 Not Failing Securely CWE-754 Improper Check for Unusual or Exceptional Conditions CWE-1088 Synchronous Access of Remote Resource without Timeout
ATT&CK	T0814 Denial of Service T0816 Device Restart/Shutdown T0880 Loss of Safety
EMB3D	TID-404 Remotely Triggerable Deadlock/DoS TID-405 Network Stack Resource Exhaustion TID-217 Remotely Initiated Updates Can Cause DoS
MDS2	SAHD System and application hardening, CSUP Cybersecurity product upgrades
Standards	IEC TR 60601-4-5 ISO 14971 IEC 62304

CRI-LS-Q Life-support alarms silenced

† CARE DELAYED OR WRONG THE PATIENT · RANK Q

THREAT

Alarm volume, limits or delays on ventilators, anaesthesia machines and dialysis can be changed through a service menu, a configuration file or a remote profile. With alarms widened or muted, disconnection, low oxygen or a pressure fault goes unnoticed until the patient deteriorates.

MITIGATION PROMPTS (ON THE CARD)

1. What is the lowest an alarm limit can be set, and by whom?
2. Can a profile, file or remote command mute a life-support alarm?
3. How would staff notice alarm settings had been widened?

MITIGATION PRINCIPLE

Alarm limits that protect life have floors that no profile, file or remote command can go below.

DESIGN MEASURES

1. Enforce non-configurable minimum alarm settings for disconnection, apnoea and low oxygen in the device itself.
2. Show a persistent indicator whenever any alarm is muted or widened, and limit mute duration.
3. Sign alarm configuration profiles and reject unsigned or out-of-range profiles at load time.

MAPPINGS

STRIDE	T Tampering, D Denial of service
CAPEC	CAPEC-176 Configuration/Environment Manipulation CAPEC-75 Manipulating Writeable Configuration Files
CWE	CWE-1188 Initialization of a Resource with an Insecure Default CWE-357 Insufficient UI Warning of Dangerous Operations
ATT&CK	T0838 Modify Alarm Settings T0878 Alarm Suppression
EMB3D	TID-224 Excessive Access via Software Diagnostic Features
MDS2	AUTH Authorization, IGAU Health data integrity and authenticity, AUDT Audit controls
Standards	IEC TR 60601-4-5 ISO 14971

CRI-LS-J Service mode open during treatment

† DIRECT HARM THE PATIENT · RANK J

THREAT

Engineering and service modes, meant for calibration and repair, can be entered while a patient is connected, by a default code, a key combination, a debug port or a remote service tool. In service mode, safety limits and interlocks may not apply.

MITIGATION PROMPTS (ON THE CARD)

1. Can service mode be entered while a patient is connected?
2. Which codes, ports or tools open service mode?
3. Which safety interlocks stop working in service mode?

MITIGATION PRINCIPLE

Service functions are unreachable while the device is delivering therapy.

DESIGN MEASURES

1. Block entry to service and calibration modes unless the device detects it is not connected to a patient.
2. Require individual, revocable service credentials, never a code shared across every unit of the model.
3. Disable or physically protect debug ports in production units and record every service-mode entry.

MAPPINGS

STRIDE	E Elevation of privilege, T Tampering
CAPEC	CAPEC-121 Exploit Non-Production Interfaces CAPEC-554 Functionality Bypass
CWE	CWE-1244 Internal Asset Exposed to Unsafe Debug Access Level or State CWE-489 Active Debug Code CWE-798 Use of Hard-coded Credentials
ATT&CK	T0858 Change Operating Mode
EMB3D	TID-224 Excessive Access via Software Diagnostic Features TID-119 Latent Hardware Debug Port Allows Memory/Code Manipulation TID-328 Hardcoded Credentials
MDS2	AUTH Authorization, PLOK Physical locks, RMOT Remote service
Standards	IEC TR 60601-4-5 AAMI SW96

CRI-LS-10 Anaesthesia workstation compromised

† DIRECT HARM THE PATIENT · RANK 10

THREAT

Anaesthesia workstations run general-purpose operating systems and connect to the anaesthesia record and the network. Malware or tampering can change gas and agent delivery, freeze the displayed values, or falsify the anaesthesia record that later decisions rely on.

MITIGATION PROMPTS (ON THE CARD)

1. Is gas and agent delivery independent of the networked computer?
2. What would a frozen display look like to the anaesthetist?
3. How is the anaesthesia record protected from later tampering?

MITIGATION PRINCIPLE

Gas and agent delivery are controlled independently of the networked computer that displays and records them.

DESIGN MEASURES

1. Keep delivery control on a separate, minimal controller that the record-keeping computer cannot command.
2. Cross-check displayed and recorded values against an independent sensor and alarm on disagreement.
3. Harden and allow-list the workstation software, and keep it on a segmented clinical device network.

MAPPINGS

STRIDE	T Tampering, I Information disclosure, D Denial of service
CAPEC	CAPEC-441 Malicious Logic Insertion CAPEC-148 Content Spoofing
CWE	CWE-1357 Reliance on Insufficiently Trustworthy Component CWE-451 User Interface (UI) Misrepresentation of Critical Information
ATT&CK	T0832 Manipulation of View T0831 Manipulation of Control
EMB3D	TID-204 Untrusted Programs Can Access Privileged OS Functions TID-205 Existing OS Tools Maliciously Used for Device Manipulation
MDS2	MLDP Malware detection and protection, SAHD System and application hardening, IGAU Health data integrity and authenticity
Standards	IEC TR 60601-4-5 IEC 80001-1

CRI-LS-9 Oxygen delivered differs from shown

† DIRECT HARM THE PATIENT · RANK 9

THREAT

Connected oxygen blenders, high-flow systems and concentrators report flow and oxygen fraction from the same software that controls them. If that software is altered, the patient receives less oxygen than the display and the record say, and hypoxia is blamed on the illness.

MITIGATION PROMPTS (ON THE CARD)

1. What measures delivered oxygen independently of the controlling software?
2. Would anyone notice the display overstating oxygen delivered?
3. Who checks that set and measured oxygen agree?

MITIGATION PRINCIPLE

Delivered oxygen is measured independently of the component that sets it.

DESIGN MEASURES

1. Measure delivered oxygen with a separate sensor and alarm when it departs from the set value.
2. Verify firmware integrity at boot and refuse to run altered control software.
3. For remotely managed home concentrators, restrict the manufacturer's cloud to reading status, not changing flow.

MAPPINGS

STRIDE	T Tampering, R Repudiation
CAPEC	CAPEC-148 Content Spoofing CAPEC-186 Malicious Software Update
CWE	CWE-353 Missing Support for Integrity Check CWE-494 Download of Code Without Integrity Check
ATT&CK	T0832 Manipulation of View T0836 Modify Parameter
EMB3D	TID-201 Inadequate Bootloader Protection and Verification TID-211 Device Allows Unauthenticated Firmware Installation
MDS2	IGAU Health data integrity and authenticity, CSUP Cybersecurity product upgrades
Standards	IEC TR 60601-4-5 ISO 14971

CRI-LS-8 Defibrillator ready status falsified

† DIRECT HARM THE PATIENT · RANK 8

THREAT

Defibrillators and public-access AEDs report self-test results, battery and pad status to fleet dashboards. A tampered device or dashboard can show ready when the unit will not charge or shock, so the failure is found only during a cardiac arrest.

MITIGATION PROMPTS (ON THE CARD)

1. How does the fleet dashboard know a defibrillator is really ready?
2. What happens when a self-test report is missing or stale?
3. Could a device show ready when it cannot charge?

MITIGATION PRINCIPLE

Readiness is reported from tamper-evident self-tests, and a missing or stale report is treated as not ready.

DESIGN MEASURES

1. Sign self-test reports on the device and verify them on the dashboard.
2. Treat missing, late or unsigned reports as a fault that triggers an inspection.
3. Keep a visible local readiness indicator that does not depend on the fleet service.

MAPPINGS

STRIDE	S Spoofing, T Tampering
CAPEC	CAPEC-194 Fake the Source of Data CAPEC-148 Content Spoofing
CWE	CWE-353 Missing Support for Integrity Check CWE-924 Improper Enforcement of Message Integrity During Transmission in a Communication Channel
ATT&CK	T0832 Manipulation of View
EMB3D	TID-407 Missing Message Replay Protection TID-406 Unauthorized Messages or Connections
MDS2	IGAU Health data integrity and authenticity, TXIG Transmission integrity, NAUT Node authentication
Standards	IEC TR 60601-4-5

CRI-LS-7 Dialysis prescription tampered

† DIRECT HARM THE PATIENT · RANK 7

THREAT

Dialysis machines load the patient's prescription, dialysate composition and fluid removal targets from a clinic system or a patient card. An altered prescription or card can remove too much fluid or deliver dialysate at the wrong conductivity or temperature.

MITIGATION PROMPTS (ON THE CARD)

1. Where does the dialysis machine load its prescription from?
2. How is a prescription checked against safe ranges before treatment?
3. Could an altered patient card change fluid removal targets?

MITIGATION PRINCIPLE

Prescriptions loaded into a dialysis machine are authenticated and checked against safe ranges before treatment starts.

DESIGN MEASURES

1. Sign prescriptions in the clinic system and verify the signature on the machine.
2. Hard-code physiological limits for conductivity, temperature and fluid removal that a prescription cannot exceed.
3. Show the loaded prescription for a nurse to confirm against the order before starting.

MAPPINGS

STRIDE	T Tampering, S Spoofing
CAPEC	CAPEC-153 Input Data Manipulation CAPEC-165 File Manipulation
CWE	CWE-353 Missing Support for Integrity Check CWE-1284 Improper Validation of Specified Quantity in Input
ATT&CK	T0836 Modify Parameter T1565.002 Transmitted Data Manipulation
EMB3D	TID-111 Untrusted External Storage
MDS2	IGAU Health data integrity and authenticity, NAUT Node authentication, AUTH Authorization
Standards	IEC TR 60601-4-5 ISO 14971

CRI-LS-6 Surgical robot command link disrupted

† DIRECT HARM THE PATIENT · RANK 6

THREAT

A surgical robot's console sends motion commands to the arms over a cable, a network or, in remote surgery, a wide-area link. Injected, delayed or dropped commands can move an instrument inside the patient or stall it mid-procedure.

MITIGATION PROMPTS (ON THE CARD)

1. How are motion commands between console and arms protected?
2. What do the arms do when commands are delayed or lost?
3. Which links does remote surgery depend on, and who runs them?

MITIGATION PRINCIPLE

Every motion command is authenticated, fresh and checked, and the arms stop safely when the link is in doubt.

DESIGN MEASURES

1. Authenticate and sequence-number every command between console and arms, rejecting stale or replayed messages.
2. Stop motion and hold position safely when latency or loss exceeds a validated limit.
3. Run remote surgery only over dedicated links with monitored quality and a local surgeon able to take over.

MAPPINGS

STRIDE	T Tampering, D Denial of service, S Spoofing
CAPEC	CAPEC-94 Adversary in the Middle (AiTM) CAPEC-60 Reusing Session IDs (aka Session Replay)
CWE	CWE-294 Authentication Bypass by Capture-replay CWE-924 Improper Enforcement of Message Integrity During Transmission in a Communication Channel
ATT&CK	T0830 Adversary-in-the-Middle T0831 Manipulation of Control
EMB3D	TID-407 Missing Message Replay Protection TID-221 Authentication Bypass By Message Replay
MDS2	TXIG Transmission integrity, NAUT Node authentication
Standards	IEC TR 60601-4-5 ISO 14971

CRI-LS-5 Neonatal incubator environment altered

† DIRECT HARM THE PATIENT · RANK 5

THREAT

Networked incubators and warmers control air temperature, humidity and oxygen for premature babies and report them to a central station. Altered control or false readings can overheat, chill or over-oxygenate a baby who cannot signal distress.

MITIGATION PROMPTS (ON THE CARD)

1. Where are temperature and oxygen limits enforced for the baby?
2. Does an independent sensor confirm the incubator's readings?
3. What would the central station show if control were altered?

MITIGATION PRINCIPLE

Environmental limits for neonates are enforced in the incubator and verified by an independent sensor.

DESIGN MEASURES

1. Enforce fixed upper and lower temperature and oxygen limits in the incubator's own controller.
2. Use an independent probe on the baby that alarms locally when it disagrees with the control sensor.
3. Make central station connections read-only for environmental settings.

MAPPINGS

STRIDE	T Tampering, D Denial of service
CAPEC	CAPEC-137 Parameter Injection CAPEC-148 Content Spoofing
CWE	CWE-862 Missing Authorization CWE-1284 Improper Validation of Specified Quantity in Input
ATT&CK	T0836 Modify Parameter T0832 Manipulation of View
EMB3D	TID-406 Unauthorized Messages or Connections
MDS2	AUTH Authorization, IGAU Health data integrity and authenticity
Standards	IEC TR 60601-4-5 ISO 14971

CRI-LS-4 Consumable checks that block therapy

† DIRECT HARM THE PATIENT · RANK 4

THREAT

Devices that authenticate circuits, cartridges, filters or licences refuse to run when the check fails, the licence server is unreachable or the clock is wrong. An attacker, an outage or a supplier change can stop ventilation, dialysis or surgery when no approved consumable is accepted.

MITIGATION PROMPTS (ON THE CARD)

1. What happens to therapy if a consumable or licence check fails?
2. Which outages could make the device refuse an approved consumable?
3. Does a failed check warn and record, or stop treatment?

MITIGATION PRINCIPLE

Consumable and licence checks never stop life-sustaining therapy; they warn and record instead.

DESIGN MEASURES

1. Let therapy continue with a clear warning and a log entry when a consumable or licence check fails.
2. Never make therapy depend on reaching a remote licence or activation service.
3. Document a clinical override for emergencies and test it during verification.

MAPPINGS

STRIDE	D Denial of service
CAPEC	CAPEC-607 Obstruction
CWE	CWE-636 Not Failing Securely CWE-1357 Reliance on Insufficiently Trustworthy Component
ATT&CK	T0813 Denial of Control T0814 Denial of Service
EMB3D	TID-222 Critical System Service May Be Disabled
MDS2	EMRG Emergency access, RDMP Roadmap for third-party components
Standards	ISO 14971 IEC TR 60601-4-5

CRI-LS-3 Setting history that proves nothing

THE PATIENT · RANK 3

THREAT

Life-support devices keep setting and event logs that are unsigned, editable by service tools, or stamped by an unsynchronised clock. After an incident nobody can tell whether a setting was changed by a clinician, a fault or an attacker, so the cause is never found.

MITIGATION PROMPTS (ON THE CARD)

1. Are device event logs signed and protected from service tools?
2. Could investigators tell a clinician's change from an attacker's?
3. Which clock stamps the setting history?

MITIGATION PRINCIPLE

Device event logs are complete, tamper-evident and trustworthy in time.

DESIGN MEASURES

1. Sign or hash-chain event logs on the device and protect them from service-tool edits.
2. Synchronise device clocks to a trusted hospital time source and record clock changes.
3. Export logs automatically to a central store the device cannot rewrite.

MAPPINGS

STRIDE	R Repudiation
LINDDUN	Nr Non-repudiation
CAPEC	CAPEC-268 Audit Log Manipulation
CWE	CWE-778 Insufficient Logging CWE-117 Improper Output Neutralization for Logs
ATT&CK	T0872 Indicator Removal on Host
EMB3D	TID-225 Logs can be manipulated on the device
MDS2	AUDT Audit controls, IGAU Health data integrity and authenticity
Standards	IEC TR 60601-4-5 AAMI SW96

CRI-LS-2 Service log exports leak patients

THE PATIENT · RANK 2

THREAT

Service and error logs exported from ventilators, anaesthesia machines and dialysis units for vendor support include patient identifiers, settings and timestamps. Sent by email or left on service laptops, they disclose patient data outside the hospital.

MITIGATION PROMPTS (ON THE CARD)

1. What patient data is in exported service logs?
2. Where do exported logs travel, and who keeps them?
3. Can identifiers be removed before logs leave the device?

MITIGATION PRINCIPLE

Logs leaving the device carry only what the vendor needs, with patient identifiers removed.

DESIGN MEASURES

1. Strip or pseudonymise patient identifiers in every log export by default.
2. Encrypt exported logs and send them through an approved, audited channel.
3. Document in the security guide exactly what each export contains.

MAPPINGS

STRIDE	I Information disclosure
LINDDUN	DD Data disclosure, I Identifying, U Unawareness and unintervenability
CAPEC	CAPEC-497 File Discovery
CWE	CWE-532 Insertion of Sensitive Information into Log File CWE-359 Exposure of Private Personal Information to an Unauthorized Actor
ATT&CK	T1005 Data from Local System
EMB3D	TID-226 Device leaks security information in logs
MDS2	DIDT Health data de-identification, STCF Data storage confidentiality, MPII Management of private data
Standards	IEC 80001-1 ISO 27799

CRI-MD · THE PATIENT · 13 ENTRIES

Medication Delivery

Infusion and PCA pumps, drug libraries, pump-EHR auto-programming, barcode administration, dispensing cabinets, pharmacy robots and controlled drug records.

https://ostering.com/taxonomies/hospitals-and-medical-devices/medication-delivery/

CRI-MD-A Drug library limits rewritten fleet-wide

† DIRECT HARM THE PATIENT · RANK A

THREAT

Drug libraries set the concentrations and hard dose limits for every infusion pump and are pushed to the whole fleet from one server. A tampered library raises or removes limits on every pump at once, so overdoses become possible across the hospital with no error on screen.

MITIGATION PROMPTS (ON THE CARD)

1. Who can change the drug library, and who reviews each change?
2. How does a pump know a library came from pharmacy unchanged?
3. Would a raised hard limit show anywhere before a patient is harmed?

MITIGATION PRINCIPLE

Drug libraries are authenticated end to end and every change is reviewed by pharmacy before it reaches a pump.

DESIGN MEASURES

1. Sign approved libraries in the pharmacy tool and have pumps verify the signature before loading.
2. Require two-person pharmacy approval for any change that raises or removes a hard limit.
3. Show the library version on each pump and alert centrally when pumps run an unapproved version.

MAPPINGS

STRIDE	T Tampering, E Elevation of privilege
CAPEC	CAPEC-186 Malicious Software Update CAPEC-75 Manipulating Writeable Configuration Files
CWE	CWE-353 Missing Support for Integrity Check CWE-494 Download of Code Without Integrity Check
ATT&CK	T0836 Modify Parameter T0889 Modify Program
EMB3D	TID-213 Faulty FW/SW Update Integrity Verification
MDS2	IGAU Health data integrity and authenticity, CSUP Cybersecurity product upgrades, AUTH Authorization
Standards	IEC 80001-1 FDA premarket

CRI-MD-K Infusion pump reprogrammed over network

† DIRECT HARM THE PATIENT · RANK K

THREAT

An infusion pump that accepts commands over Wi-Fi or Ethernet without strong authentication can have its rate, volume or drug changed, or be stopped, by anyone on the network. The pump may show the change as a normal programme.

MITIGATION PROMPTS (ON THE CARD)

1. Which systems can send commands to a pump over the network?
2. Can a rate or drug change without a clinician at the pump?
3. How would a remote change look different from a normal programme?

SEEN IN PUBLIC

Hospira Symbiq infusion pumps, 2015. The FDA advised hospitals to stop using Hospira Symbiq infusion pumps because they could be accessed remotely over the hospital network and their dosing changed. Sources: MDDI: FDA, stop using infusion pump vulnerable to hacking

MITIGATION PRINCIPLE

Pumps accept network commands only from authenticated systems, and dose changes need a clinician at the pump.

DESIGN MEASURES

1. Mutually authenticate the pump and its server, and refuse all commands from anything else.
2. Disable network services the clinical workflow does not use, such as remote shells or diagnostic ports.
3. Require confirmation at the pump for any change to rate, volume or drug.

MAPPINGS

STRIDE	S Spoofing, T Tampering, E Elevation of privilege
CAPEC	CAPEC-151 Identity Spoofing CAPEC-137 Parameter Injection
CWE	CWE-306 Missing Authentication for Critical Functionality CWE-798 Use of Hard-coded Credentials
ATT&CK	T0836 Modify Parameter T0886 Remote Services
EMB3D	TID-310 Remotely Accessible Unauthenticated Services TID-328 Hardcoded Credentials
MDS2	NAUT Node authentication, AUTH Authorization, SAHD System and application hardening
Standards	IEC TR 60601-4-5 FDA premarket

CRI-MD-Q Unsigned pump firmware accepted

† DIRECT HARM THE PATIENT · RANK Q

THREAT

Pumps that install firmware without verifying who built it can be given modified software through the update server, a service laptop or a USB port. Altered firmware can change dose calculation or alarms on every pump that takes the update.

MITIGATION PROMPTS (ON THE CARD)

1. Where does the pump verify that firmware is genuine?
2. Which routes can deliver firmware: update server, laptop, USB?
3. How many pumps would one bad update reach?

MITIGATION PRINCIPLE

Pumps run only firmware signed by the manufacturer and verified on the device.

DESIGN MEASURES

1. Verify a manufacturer signature at install and at every boot, with the key held in hardware.
2. Block rollback to older, vulnerable firmware versions.
3. Restrict update installation to an authenticated, logged service path.

MAPPINGS

STRIDE	T Tampering, E Elevation of privilege
CAPEC	CAPEC-186 Malicious Software Update CAPEC-533 Malicious Manual Software Update
CWE	CWE-494 Download of Code Without Integrity Check CWE-347 Improper Verification of Cryptographic Signature
ATT&CK	T0800 Activate Firmware Update Mode T0862 Supply Chain Compromise
EMB3D	TID-211 Device Allows Unauthenticated Firmware Installation TID-213 Faulty FW/SW Update Integrity Verification TID-216 Firmware Update Rollbacks Allowed
MDS2	CSUP Cybersecurity product upgrades, IGAU Health data integrity and authenticity
Standards	IEC TR 60601-4-5 FDA premarket AAMI SW96

CRI-MD-J Auto-programming sends a wrong dose

† DIRECT HARM THE PATIENT · RANK J

THREAT

When the EHR programmes the pump directly from the order, nurses learn to trust the prefilled values. A tampered message, a mapping error between order units and pump units, or a spoofed integration server can load the wrong drug, rate or patient.

MITIGATION PROMPTS (ON THE CARD)

1. How is an auto-programming message authenticated between EHR and pump?
2. Where could order units and pump units be mapped wrongly?
3. What makes the nurse check prefilled values against the order?

MITIGATION PRINCIPLE

Pump-EHR messages are authenticated and every auto-programmed infusion is checked by a person against the order.

DESIGN MEASURES

1. Authenticate and integrity-protect messages between the EHR, the interoperability server and the pump.
2. Match patient, drug and concentration by scanned identifiers before the programme is accepted.
3. Show the full programme at the pump and require confirmation; never start automatically.

MAPPINGS

STRIDE	S Spoofing, T Tampering
CAPEC	CAPEC-94 Adversary in the Middle (AiTM) CAPEC-148 Content Spoofing
CWE	CWE-353 Missing Support for Integrity Check CWE-924 Improper Enforcement of Message Integrity During Transmission in a Communication Channel
ATT&CK	T1565.002 Transmitted Data Manipulation T0830 Adversary-in-the-Middle
EMB3D	TID-406 Unauthorized Messages or Connections
MDS2	TXIG Transmission integrity, NAUT Node authentication, IGAU Health data integrity and authenticity
Standards	IEC 80001-1 IEC TR 60601-4-5

CRI-MD-10 PCA limits loosened

† DIRECT HARM THE PATIENT · RANK 10

THREAT

Patient-controlled analgesia pumps let patients give themselves opioid doses within a lockout and hourly limit. If those limits can be changed remotely, by a shared clinician code or through a weak key lock, a patient can receive a fatal dose.

MITIGATION PROMPTS (ON THE CARD)

1. Who can change PCA lockout and hourly limits, and how?
2. Are clinician codes on PCA pumps individual or shared?
3. What bounds does pharmacy set that no one can exceed?

MITIGATION PRINCIPLE

PCA limits change only with individual clinician authentication at the pump and stay within pharmacy-approved bounds.

DESIGN MEASURES

1. Require individual clinician authentication at the pump to change PCA limits.
2. Enforce library hard limits on lockout and hourly dose that the bedside cannot override.
3. Use a physical lock for the drug reservoir and alarm on door opening.

MAPPINGS

STRIDE	T Tampering, E Elevation of privilege
CAPEC	CAPEC-122 Privilege Abuse CAPEC-391 Bypassing Physical Locks
CWE	CWE-1391 Use of Weak Credentials CWE-1263 Improper Physical Access Control
ATT&CK	T0836 Modify Parameter
EMB3D	TID-311 Default Credentials
MDS2	PAUT Person authentication, AUTH Authorization, PLOK Physical locks
Standards	IEC TR 60601-4-5

CRI-MD-9 Barcode checks quietly bypassed

† DIRECT HARM THE PATIENT · RANK 9

THREAT

Barcode medication administration only protects patients when the scans are real. Relabelled drugs, copied wristbands, a scanner that accepts typed numbers, or a degraded mode that skips checks during an outage lets the wrong drug reach the wrong patient.

MITIGATION PROMPTS (ON THE CARD)

1. Can a scanner accept a typed number instead of a scan?
2. What happens to bedside checks when the system is down?
3. How would copied wristbands or relabelled drugs be caught?

MITIGATION PRINCIPLE

Bedside checks depend on scanned identifiers that cannot be typed or copied, and degraded modes are visible and recorded.

DESIGN MEASURES

1. Disable manual entry of drug and patient identifiers, or require a second clinician to witness it.
2. Make any bypass or degraded mode visible on the ward and report bypass rates daily.
3. Use tamper-evident wristbands and verify barcodes against the pharmacy dispensing record.

MAPPINGS

STRIDE	S Spoofing, T Tampering, R Repudiation
CAPEC	CAPEC-148 Content Spoofing CAPEC-554 Functionality Bypass
CWE	CWE-807 Reliance on Untrusted Inputs in a Security Decision CWE-602 Client-Side Enforcement of Server-Side Security
ATT&CK	T1036 Masquerading
MDS2	AUDT Audit controls, IGAU Health data integrity and authenticity
Standards	IEC 80001-1

CRI-MD-8 Compounding robot recipes altered

† DIRECT HARM THE PATIENT · RANK 8

THREAT

Pharmacy robots and compounding systems prepare chemotherapy, parenteral nutrition and syringes from stored recipes and the order feed. An altered recipe or calibration produces many wrong-strength doses that look correctly labelled.

MITIGATION PROMPTS (ON THE CARD)

1. Who controls changes to compounding recipes and calibration?
2. How is a prepared dose checked independently of the robot?
3. How many doses would one altered recipe affect before anyone noticed?

MITIGATION PRINCIPLE

Recipes and calibration in compounding systems are controlled documents, and outputs are verified independently.

DESIGN MEASURES

1. Sign recipes and require pharmacist approval for each change, with version history.
2. Verify each preparation by gravimetric or analytical check independent of the robot's own software.
3. Restrict the robot's network access to the pharmacy system it serves.

MAPPINGS

STRIDE	T Tampering
CAPEC	CAPEC-176 Configuration/Environment Manipulation CAPEC-165 File Manipulation
CWE	CWE-353 Missing Support for Integrity Check CWE-732 Incorrect Permission Assignment for Critical Resource
ATT&CK	T0836 Modify Parameter T1565.001 Stored Data Manipulation
MDS2	IGAU Health data integrity and authenticity, AUTH Authorization, AUDT Audit controls
Standards	IEC 80001-1

CRI-MD-7 Pumps report infusing when stopped

† DIRECT HARM · THE PATIENT · RANK 7

THREAT

Central infusion views and alarm routing depend on status messages from pumps. A flood of traffic, a crashed pump stack or a forged status can stop an infusion of a vasoactive or sedative drug while the ward screen still shows it running.

MITIGATION PROMPTS (ON THE CARD)

1. How does the ward know an infusion has really stopped?
2. Does the pump alarm locally, or only through the network?
3. Could a forged status hide a stopped vasoactive infusion?

SEEN IN PUBLIC

URGENT/11, 2019. The FDA warned that 11 vulnerabilities in IPnet, a third-party network stack inside several embedded operating systems, could let attackers take over or crash medical devices and hospital network equipment, and that manufacturers might not know their products contained it.
Sources: Healthcare IT News: URGENT/11, FDA issues alert

MITIGATION PRINCIPLE

Loss of infusion is detected and alarmed at the pump, not inferred from network status.

DESIGN MEASURES

1. Alarm locally at the pump on any stop or occlusion, independent of the network.
2. Show stale or missing pump status as unknown at the central view, never as the last good value.
3. Test pump network stacks against flooding and malformed traffic.

MAPPINGS

STRIDE	D Denial of service, S Spoofing
CAPEC	CAPEC-125 Flooding CAPEC-194 Fake the Source of Data
CWE	CWE-770 Allocation of Resources Without Limits or Throttling CWE-392 Missing Report of Error Condition
ATT&CK	T0815 Denial of View T0814 Denial of Service
EMB3D	TID-405 Network Stack Resource Exhaustion TID-202 Exploitable System Network Stack Component
MDS2	TXIG Transmission integrity, SAHD System and application hardening
Standards	IEC 80001-1 IEC TR 60601-4-5

CRI-MD-6 Dispensing cabinets fail closed

† CARE DELAYED OR WRONG · THE PATIENT · RANK 6

THREAT

Automated dispensing cabinets unlock drawers only after checking orders and users with a central server. During a network outage or ransomware the cabinets lock, and emergency drugs are out of reach on the ward.

MITIGATION PROMPTS (ON THE CARD)

1. Can staff reach emergency drugs when the cabinet server is down?
2. How is offline cabinet access recorded and reconciled later?
3. When was cabinet failure last rehearsed on a ward?

MITIGATION PRINCIPLE

Cabinets keep emergency drugs available offline, with access recorded for later reconciliation.

DESIGN MEASURES

1. Hold a cached order and user list on each cabinet with an offline emergency mode.
2. Keep a sealed emergency key procedure and practise it in downtime drills.
3. Record all offline access locally and reconcile it when the server returns.

MAPPINGS

STRIDE	D Denial of service
CAPEC	CAPEC-607 Obstruction
CWE	CWE-636 Not Failing Securely
ATT&CK	T0826 Loss of Availability T0813 Denial of Control
MDS2	EMRG Emergency access, DTBK Data backup and disaster recovery
Standards	IEC 80001-1

CRI-MD-5 Pharmacy labels misprinted

† CARE DELAYED OR WRONG THE PATIENT · RANK 5

THREAT

Labels for prepared doses and patient medication are printed from pharmacy systems through shared print queues. Altered label templates or queue tampering can print the wrong strength, route or patient on correctly prepared doses.

MITIGATION PROMPTS (ON THE CARD)

1. Where are label templates kept, and who can change them?
2. Is the printed label checked against the dispensing record?
3. Who else shares the print queues that pharmacy labels use?

MITIGATION PRINCIPLE

What is printed on a label is generated and checked from the verified dispensing record.

DESIGN MEASURES

1. Print labels only from the verified dispensing record, with the label content signed or check-summed.
2. Isolate pharmacy label printers from general print queues.
3. Scan the printed label back against the record before release.

MAPPINGS

STRIDE	T Tampering
CAPEC	CAPEC-148 Content Spoofing CAPEC-75 Manipulating Writeable Configuration Files
CWE	CWE-353 Missing Support for Integrity Check
ATT&CK	T1565.001 Stored Data Manipulation
MDS2	IGAU Health data integrity and authenticity

CRI-MD-4 Controlled drug records falsified

THE PATIENT · RANK 4

THREAT

Electronic controlled-drug registers and cabinet logs can be edited by privileged users, shared accounts or service tools. Diversion of opioids is hidden, patients get substituted or short doses, and investigations cannot show who took what.

MITIGATION PROMPTS (ON THE CARD)

1. Can every controlled drug entry be traced to one person?
2. Who can edit the register, including service tools?
3. How would opioid diversion show up in these records?

MITIGATION PRINCIPLE

Controlled drug records are attributable to individuals and cannot be changed without trace.

DESIGN MEASURES

1. Require individual authentication and a witness for every controlled-drug transaction.
2. Make the register append-only, with corrections as new entries.
3. Analyse transactions for diversion patterns and review them routinely.

MAPPINGS

STRIDE	R Repudiation, T Tampering
LINDDUN	Nr Non-repudiation
CAPEC	CAPEC-268 Audit Log Manipulation CAPEC-122 Privilege Abuse
CWE	CWE-778 Insufficient Logging CWE-862 Missing Authorization
ATT&CK	T1565.001 Stored Data Manipulation T1078 Valid Accounts
MDS2	AUDT Audit controls, PAUT Person authentication, AUTH Authorization

CRI-MD-3 Pumps run stale drug libraries

† DIRECT HARM THE PATIENT · RANK 3

THREAT

Pumps that are off the network, in storage or on loan never receive library updates, and nothing reports which version each pump holds. A withdrawn concentration or an unsafe old limit stays in use without anyone knowing.

MITIGATION PROMPTS (ON THE CARD)

1. How do you know which library version each pump holds?
2. What happens to pumps in storage or on loan when libraries change?
3. Can a pump with an outdated library still be used on a patient?

MITIGATION PRINCIPLE

Every pump's library version is known, and outdated pumps are kept out of use.

DESIGN MEASURES

1. Report each pump's library version centrally and flag pumps that have not checked in.
2. Block programming from a library older than an approved minimum version.
3. Include library checks in the process for pumps returning from storage, repair or loan.

MAPPINGS

STRIDE	T Tampering
CAPEC	CAPEC-176 Configuration/Environment Manipulation
CWE	CWE-672 Operation on a Resource after Expiration or Release
EMB3D	TID-210 Device Vulnerabilities Unpatchable
MDS2	CSUP Cybersecurity product upgrades
Standards	IEC 80001-1

CRI-MD-2 Infusion history leaks patient data

THE PATIENT · RANK 2

THREAT

Pumps and their servers keep infusion histories with drug, dose, time and often patient identifiers. Transmitted in clear, stored unencrypted on the pump, or left on decommissioned units, they reveal sensitive treatments such as chemotherapy or HIV therapy.

MITIGATION PROMPTS (ON THE CARD)

1. What patient details do pumps keep in their infusion history?
2. Is infusion history encrypted on the pump and in transit?
3. What is wiped before a pump leaves the hospital?

MITIGATION PRINCIPLE

Infusion histories are minimised, encrypted and wiped when a pump leaves service.

DESIGN MEASURES

1. Encrypt pump data at rest and in transit to the server.
2. Keep only the identifiers the workflow needs on the pump itself.
3. Wipe pumps verifiably before repair, resale or disposal.

MAPPINGS

STRIDE	I Information disclosure
LINDDUN	DD Data disclosure, I Identifying, L Linking
CAPEC	CAPEC-117 Interception CAPEC-675 Retrieve Data from Decommissioned Devices
CWE	CWE-319 Cleartext Transmission of Sensitive Information CWE-359 Exposure of Private Personal Information to an Unauthorized Actor CWE-226 Sensitive Information in Resource Not Removed Before Reuse
ATT&CK	T0882 Theft of Operational Information
EMB3D	TID-408 Unencrypted Sensitive Data Communication TID-108 ROM/NVRAM Data Extraction or Modification
MDS2	STCF Data storage confidentiality, TXCF Transmission confidentiality, MPII Management of private data
Standards	IEC 80001-1 ISO 27799

CRI-IR · THE PATIENT · 13 ENTRIES

Imaging and Radiation

X-ray, CT, MRI, fluoroscopy, ultrasound, mammography, nuclear medicine and radiotherapy, with their worklists, workstations, images and dose.

https://ostering.com/taxonomies/hospitals-and-medical-devices/imaging-and-radiation/

CRI-IR-A Radiotherapy plan altered before delivery

† DIRECT HARM THE PATIENT · RANK A

THREAT

Treatment plans pass from the planning system through the oncology information system to the linac. A changed dose, field shape, gantry angle or patient position between approval and delivery can give a serious overdose or miss the tumour, and harm may appear only weeks later.

MITIGATION PROMPTS (ON THE CARD)

1. How do you prove the plan delivered matches the plan approved?
2. Which systems can change a plan between approval and the linac?
3. Would a changed field or dose be caught before the first fraction?

MITIGATION PRINCIPLE

The plan delivered is provably the plan the clinicians approved.

DESIGN MEASURES

1. Sign the approved plan in the planning system and verify the signature at the treatment console.
2. Run independent dose verification of the delivered plan before the first fraction.
3. Log every plan modification with user and reason, and alert on changes after approval.

MAPPINGS

STRIDE	T Tampering, R Repudiation
CAPEC	CAPEC-165 File Manipulation CAPEC-148 Content Spoofing
CWE	CWE-353 Missing Support for Integrity Check CWE-354 Improper Validation of Integrity Check Value
ATT&CK	T1565.001 Stored Data Manipulation T0836 Modify Parameter
MDS2	IGAU Health data integrity and authenticity, AUDT Audit controls, NAUT Node authentication
Standards	IEC 80001-1 IEC 62304

CRI-IR-K Radiotherapy service halted

† CARE DELAYED OR WRONG THE PATIENT · RANK K

THREAT

Linacs depend on planning systems, oncology information systems and, increasingly, vendor-hosted cloud services. Ransomware at the hospital or the vendor stops treatment courses that must not be interrupted, and patients' cancers progress.

MITIGATION PROMPTS (ON THE CARD)

1. How long can radiotherapy continue without its planning and cloud systems?
2. Which vendor services does treatment delivery depend on?
3. Who decides which patients' courses continue during an outage?

SEEN IN PUBLIC

Elekta cloud outage, 2021. Ransomware hit Elekta's first-generation US cloud service for radiation oncology software, and about 170 US health systems were affected; some cancer centres could not treat patients for over a week because treatment programming was held in the cloud. Sources: Compliancy Group: Healthcare vendor ransomware attack, 170 health systems hit; Yale Daily News: YNHHS pauses radiotherapy treatment for six days

MITIGATION PRINCIPLE

Radiotherapy can continue safely for a defined period when its supporting systems are lost.

DESIGN MEASURES

1. Hold an offline, verified copy of active treatment plans and schedules for each linac.
2. Plan and rehearse transfer of patients to partner centres with compatible equipment.
3. Require vendors to document continuity for cloud-hosted components in the contract.

MAPPINGS

STRIDE	D Denial of service
CAPEC	CAPEC-607 Obstruction
CWE	CWE-1357 Reliance on Insufficiently Trustworthy Component
ATT&CK	T1486 Data Encrypted for Impact T1490 Inhibit System Recovery
MDS2	DTBK Data backup and disaster recovery, RDMP Roadmap for third-party components
Standards	IEC 80001-1

CRI-IR-Q Image tampering adds or removes findings

† CARE DELAYED OR WRONG THE PATIENT · RANK Q

THREAT

Images move from scanner to archive to reporting workstation, often without integrity protection. An attacker can add or remove a tumour, bleed or fracture in CT, MRI or X-ray images, leading to unnecessary surgery or missed treatment that radiologists cannot detect by eye.

MITIGATION PROMPTS (ON THE CARD)

1. Where are images integrity-protected between scanner and reporting?
2. Could a radiologist tell that a finding had been added or removed?
3. Who can write to the image archive?

MITIGATION PRINCIPLE

Diagnostic images are integrity-protected from acquisition to reporting.

DESIGN MEASURES

1. Sign or hash images at the modality and verify them in the archive and on the viewer.
2. Use TLS for all DICOM transfers inside the hospital, not only external ones.
3. Alert when an image object is modified after acquisition and keep the original.

MAPPINGS

STRIDE	T Tampering
CAPEC	CAPEC-148 Content Spoofing CAPEC-94 Adversary in the Middle (AiTM)
CWE	CWE-353 Missing Support for Integrity Check CWE-319 Cleartext Transmission of Sensitive Information
ATT&CK	T1565.002 Transmitted Data Manipulation T1565.001 Stored Data Manipulation
EMB3D	TID-408 Unencrypted Sensitive Data Communication
MDS2	IGAU Health data integrity and authenticity, TXIG Transmission integrity
Standards	DICOM PS3.15 IEC 80001-1

CRI-IR-J Imaging dose protocols raised

† DIRECT HARM THE PATIENT · RANK J

THREAT

CT, fluoroscopy, mammography and X-ray dose depends on protocol libraries pushed to scanners. A tampered protocol raises tube current or exposure time across many patients, and the extra radiation is not noticed until audits or injuries appear.

MITIGATION PROMPTS (ON THE CARD)

1. Who can change scanner dose protocols, and is it reviewed?
2. How is dose outside reference levels caught at the scanner?
3. How long would raised doses go unnoticed across many patients?

MITIGATION PRINCIPLE

Dose protocols are controlled, and dose outside reference levels is caught at the scanner.

DESIGN MEASURES

1. Sign protocol libraries and require physicist approval for changes.
2. Enforce dose alerts and notifications at the scanner against reference levels.
3. Monitor dose records centrally and alarm on shifts in average dose per protocol.

MAPPINGS

STRIDE	T Tampering
CAPEC	CAPEC-176 Configuration/Environment Manipulation CAPEC-75 Manipulating Writeable Configuration Files
CWE	CWE-353 Missing Support for Integrity Check CWE-732 Incorrect Permission Assignment for Critical Resource
ATT&CK	T0836 Modify Parameter
MDS2	IGAU Health data integrity and authenticity, AUTH Authorization, AUDT Audit controls
Standards	IEC 80001-1

CRI-IR-10 DICOM files carry malware

THE PATIENT · RANK 10

THREAT

DICOM image files can also be valid executables, and images arrive on CDs, USB drives, shares and from other hospitals. Malware hides in patient images, and anti-malware that quarantines the file deletes clinical evidence.

MITIGATION PROMPTS (ON THE CARD)

1. Where are imported images parsed before they reach clinical workstations?
2. What happens to an image file that anti-malware flags?
3. Which routes bring outside images in: CD, USB, share, network?

SEEN IN PUBLIC

DICOM files carrying malware, 2019. Cylera researchers showed that the DICOM file format allows an image file to also be a working Windows executable, so malware could hide inside medical images protected as patient data (CVE-2019-11687). Sources: NVD: CVE-2019-11687; GovInfoSecurity: Researchers, malware can be hidden in medical images

MITIGATION PRINCIPLE

Imported images are parsed and checked in isolation before they reach clinical workstations.

DESIGN MEASURES

1. Import external media through an isolated gateway that validates DICOM structure and strips unexpected content.
2. Disable autorun and execution of files from imaging import folders.
3. Agree with the vendor how infected images are handled without losing the clinical record.

MAPPINGS

STRIDE	T Tampering, E Elevation of privilege
CAPEC	CAPEC-636 Hiding Malicious Data or Code within Files CAPEC-457 USB Memory Attacks
CWE	CWE-434 Unrestricted Upload of File with Dangerous Type CWE-1287 Improper Validation of Specified Type of Input
ATT&CK	T1204.002 Malicious File T1027.009 Embedded Payloads
EMB3D	TID-111 Untrusted External Storage
MDS2	MLDP Malware detection and protection, SAHD System and application hardening
Standards	DICOM PS3.15

CRI-IR-9 Scanners stuck on unsupported systems

† CARE DELAYED OR WRONG THE PATIENT · RANK 9

THREAT

CT, MRI and X-ray consoles often run operating systems the vendor certified years ago and that can no longer be patched. Ransomware spreading across the network shuts scanners down, and emergency imaging stops.

MITIGATION PROMPTS (ON THE CARD)

1. Which imaging consoles run operating systems that can't be patched?
2. What could reach those consoles if ransomware spread?
3. How quickly could a scanner be rebuilt and back in service?

SEEN IN PUBLIC

WannaCry and the NHS, 2017. WannaCry ransomware disrupted at least 81 of England's 236 NHS trusts and infected 595 GP practices; the NAO estimated over 19,000 appointments were cancelled, and some trusts diverted ambulances. Sources: NAO: Investigation, WannaCry cyber attack and the NHS; GOV.UK: Foreign Office Minister condemns North Korean actor for WannaCry attacks

MITIGATION PRINCIPLE

Imaging consoles that cannot be patched are isolated and kept recoverable.

DESIGN MEASURES

1. Place modalities in their own network segment allowing only DICOM traffic to named systems.
2. Require vendors to commit to supported operating system lifetimes and validated patches.
3. Keep a tested restore image for each console and practise recovery.

MAPPINGS

STRIDE	D Denial of service, E Elevation of privilege
CAPEC	CAPEC-682 Exploitation of Firmware or ROM Code with Unpatchable Vulnerabilities
CWE	CWE-1104 Use of Unmaintained Third Party Components CWE-1329 Reliance on Component That is Not Updateable
ATT&CK	T1210 Exploitation of Remote Services T1486 Data Encrypted for Impact
EMB3D	TID-210 Device Vulnerabilities Unpatchable
MDS2	RDMP Roadmap for third-party components, CSUP Cybersecurity product upgrades, SAHD System and application hardening
Standards	IEC 80001-1 AAMI SW96

CRI-IR-8 Worklist mix-up assigns wrong patient

† CARE DELAYED OR WRONG THE PATIENT · RANK 8

THREAT

Scanners take patient details from the modality worklist. A spoofed worklist server or altered entry puts images under the wrong patient, so a scan is reported for one person and acted on for another.

MITIGATION PROMPTS (ON THE CARD)

1. How does the scanner know the worklist server is genuine?
2. Where is patient identity confirmed before the scan starts?
3. How would images filed under the wrong patient be spotted?

MITIGATION PRINCIPLE

Patient identity on images comes from an authenticated worklist and is confirmed at the scanner.

DESIGN MEASURES

1. Authenticate the worklist server to the modality and restrict who can query it.
2. Confirm patient identity at the scanner against the wristband before acquisition.
3. Reconcile acquired studies with orders and flag mismatches before reporting.

MAPPINGS

STRIDE	S Spoofing, T Tampering
LINDDUN	I Identifying
CAPEC	CAPEC-151 Identity Spoofing CAPEC-194 Fake the Source of Data
CWE	CWE-290 Authentication Bypass by Spoofing CWE-346 Origin Validation Error
ATT&CK	T1557 Adversary-in-the-Middle
MDS2	NAUT Node authentication, IGAU Health data integrity and authenticity
Standards	DICOM PS3.15

CRI-IR-7 MRI safety limits overridden

† DIRECT HARM THE PATIENT · RANK 7

THREAT

MRI scanners limit gradient switching and radiofrequency energy to prevent burns and nerve stimulation, and manage helium and quench systems. Altered limits, monitoring software or service settings can burn a patient or damage the magnet.

MITIGATION PROMPTS (ON THE CARD)

1. Are MRI safety limits enforced in hardware, firmware or settings?
2. Who can change gradient, energy or quench settings?
3. What alerts staff if a safety limit has been altered?

MITIGATION PRINCIPLE

Patient safety limits in MRI are enforced in hardware or protected firmware, not configurable software.

DESIGN MEASURES

1. Enforce specific absorption rate and gradient limits in a protected controller.
2. Separate quench and cryogen monitoring from the networked console.
3. Restrict service settings to authenticated engineers with logged sessions.

MAPPINGS

STRIDE	T Tampering, E Elevation of privilege
CAPEC	CAPEC-176 Configuration/Environment Manipulation CAPEC-121 Exploit Non-Production Interfaces
CWE	CWE-1244 Internal Asset Exposed to Unsafe Debug Access Level or State CWE-863 Incorrect Authorization
ATT&CK	T0836 Modify Parameter T0837 Loss of Protection
EMB3D	TID-224 Excessive Access via Software Diagnostic Features
MDS2	AUTH Authorization, AUDT Audit controls
Standards	IEC TR 60601-4-5

CRI-IR-6 Nuclear medicine activity misrecorded

† DIRECT HARM THE PATIENT · RANK 6

THREAT

Dose calibrators and radiopharmacy software record the activity drawn for each patient. Altered calibration factors or records give patients the wrong radiation dose or invalidate scans.

MITIGATION PROMPTS (ON THE CARD)

1. How are dose calibrator calibration factors protected and checked?
2. Who can edit the activity recorded for a patient?
3. Would a wrong dose show up before administration?

MITIGATION PRINCIPLE

Radiopharmaceutical activity is measured and recorded with verified calibration.

DESIGN MEASURES

1. Protect calibration factors from change without physicist approval.
2. Check calibrators daily against a reference source and record the result.
3. Keep activity records append-only and linked to the order.

MAPPINGS

STRIDE	T Tampering, R Repudiation
CAPEC	CAPEC-165 File Manipulation
CWE	CWE-353 Missing Support for Integrity Check
ATT&CK	T1565.001 Stored Data Manipulation
MDS2	IGAU Health data integrity and authenticity, AUDT Audit controls

CRI-IR-5 Imaging archive exposed online

THE PATIENT · RANK 5

THREAT

Image archives and DICOM nodes reachable from the internet, or from guest networks, answer queries without authentication. Millions of images and reports with names and dates of birth can be downloaded.

MITIGATION PROMPTS (ON THE CARD)

1. Can the image archive be queried from the internet or guest Wi-Fi?
2. Which systems may query the archive, and how are they authenticated?
3. When did anyone last check what the archive answers to?

SEEN IN PUBLIC

Open PACS servers, 2019. Greenbone found about 590 imaging archive (PACS) servers reachable on the internet without protection, exposing records of about 24 million patients and hundreds of millions of images; an update later counted over a billion images. Sources: Help Net Security: Confidential data of 24.3 million patients discovered online; HIPAA Journal: Exposed medical image total rises to 1.19 billion

MITIGATION PRINCIPLE

Image archives answer only authenticated, authorised systems on approved networks.

DESIGN MEASURES

1. Never expose DICOM services directly to the internet; use authenticated gateways for external sharing.
2. Require node authentication and TLS for every DICOM association.
3. Scan regularly for exposed imaging services.

MAPPINGS

STRIDE	I Information disclosure
LINDDUN	DD Data disclosure, I Identifying
CAPEC	CAPEC-1 Accessing Functionality Not Properly Constrained by ACLs CAPEC-158 Sniffing Network Traffic
CWE	CWE-306 Missing Authentication for Critical Functionality CWE-359 Exposure of Private Personal Information to an Unauthorized Actor
ATT&CK	T1190 Exploit Public-Facing Application
EMB3D	TID-310 Remotely Accessible Unauthenticated Services
MDS2	NAUT Node authentication, TXCF Transmission confidentiality, AUTH Authorization
Standards	DICOM PS3.15 ISO 27799

CRI-IR-4 Image metadata re-identifies patients

THE PATIENT · RANK 4

THREAT

Images shared for research, teaching or AI training keep patient details in headers, burned-in text or the anatomy itself. Head CT and MRI can be rendered into recognisable faces, so de-identified data identifies people.

MITIGATION PROMPTS (ON THE CARD)

1. What patient details remain in images shared for research or AI?
2. Is burned-in text removed from the pixels as well as headers?
3. Could a head scan be rendered into a recognisable face?

MITIGATION PRINCIPLE

Images leaving clinical use are de-identified in headers, pixels and anatomy, and checked.

DESIGN MEASURES

1. Apply a de-identification profile that covers headers, private tags and burned-in annotations.
2. Deface head and neck studies before release.
3. Check a sample of every release for residual identifiers.

MAPPINGS

STRIDE	I Information disclosure
LINDDUN	I Identifying, L Linking, DD Data disclosure
CAPEC	CAPEC-497 File Discovery
CWE	CWE-1230 Exposure of Sensitive Information Through Metadata CWE-359 Exposure of Private Personal Information to an Unauthorized Actor
MDS2	DIDT Health data de-identification
Standards	DICOM PS3.15 ISO 27799

CRI-IR-3 Portable imaging stores images unprotected

THE PATIENT · RANK 3

THREAT

Portable ultrasound and X-ray units and handheld probes paired to phones store images locally and upload to clouds. A lost device or an unencrypted upload discloses patient images.

MITIGATION PROMPTS (ON THE CARD)

1. What images stay stored on portable units and paired phones?
2. Where do portable devices upload, and is that approved?
3. What happens to images when a handheld probe is lost?

MITIGATION PRINCIPLE

Portable imaging keeps no more data than needed, encrypted, and uploads only to approved destinations.

DESIGN MEASURES

1. Encrypt local image storage and wipe images after confirmed transfer.
2. Restrict uploads to the hospital archive or an approved, contracted service.
3. Support remote wipe and inventory for portable units and their phones.

MAPPINGS

STRIDE	I Information disclosure
LINDDUN	DD Data disclosure
CAPEC	CAPEC-507 Physical Theft
CWE	CWE-359 Exposure of Private Personal Information to an Unauthorized Actor
ATT&CK	T1005 Data from Local System
MDS2	STCF Data storage confidentiality, TXCF Transmission confidentiality, PLOK Physical locks
Standards	ISO 27799

CRI-IR-2 Viewer presets that hide findings

† CARE DELAYED OR WRONG THE PATIENT · RANK 2

THREAT

Diagnostic viewers and displays rely on window settings, presets and calibration. Altered presets or display calibration can make a subtle finding invisible, and the radiologist reports a normal study.

MITIGATION PROMPTS (ON THE CARD)

1. Who can change viewer presets and window settings?
2. How is display calibration checked, and how often?
3. Would a changed preset be visible to the radiologist?

MITIGATION PRINCIPLE

Viewer presets and display calibration are controlled and checked.

DESIGN MEASURES

1. Manage presets centrally with change control and version history.
2. Run regular display calibration checks and log results.
3. Show when a non-standard preset is in use.

MAPPINGS

STRIDE	T Tampering
CAPEC	CAPEC-176 Configuration/Environment Manipulation
CWE	CWE-451 User Interface (UI) Misrepresentation of Critical Information
ATT&CK	T1565.003 Runtime Data Manipulation
MDS2	IGAU Health data integrity and authenticity

CRI-LD · THE PATIENT · 13 ENTRIES

Laboratory and Diagnostics

Analysers, LIS and middleware, point-of-care tests, blood bank, pathology and digital pathology, sequencers and outsourced lab services.

https://ostering.com/taxonomies/hospitals-and-medical-devices/laboratory-and-diagnostics/

CRI-LD-A Results altered before reaching the record

† CARE DELAYED OR WRONG THE PATIENT · RANK A

THREAT

Analyser results pass through middleware and the laboratory information system to the record with no end-to-end integrity check. A changed potassium, troponin or glucose value is filed as genuine, and clinicians treat, discharge or withhold treatment on it.

MITIGATION PROMPTS (ON THE CARD)

1. How do you prove a result is the value the analyser measured?
2. Which systems between analyser and record could change a value?
3. Would anyone notice a plausible but altered potassium result?

MITIGATION PRINCIPLE

A result must be provably the value the analyser measured, from instrument to record.

DESIGN MEASURES

1. Sign or hash each result at the analyser or middleware and verify it before filing in the record.
2. Reconcile result counts and values between analyser logs and the record on a schedule, and alert on mismatches.
3. Restrict who and what can edit a validated result, and keep every amendment visible with its reason.

MAPPINGS

STRIDE	T Tampering
CAPEC	CAPEC-153 Input Data Manipulation CAPEC-385 Transaction or Event Tampering via Application API Manipulation
CWE	CWE-924 Improper Enforcement of Message Integrity During Transmission in a Communication Channel CWE-353 Missing Support for Integrity Check
ATT&CK	T1565.002 Transmitted Data Manipulation T1565.001 Stored Data Manipulation
MDS2	IGAU Health data integrity and authenticity, TXIG Transmission integrity, AUDT Audit controls
Standards	IEC 81001-5-1 IEC 80001-1

CRI-LD-K Blood matched to the wrong patient

† DIRECT HARM THE PATIENT · RANK K

THREAT

Blood bank systems trust the group, antibody results and sample labels they are given. A changed group, a swapped sample identity or a forged crossmatch release leads to an incompatible transfusion, which can kill within minutes.

MITIGATION PROMPTS (ON THE CARD)

1. Which records must agree before blood is released for a patient?
2. Could one person or system change a group or crossmatch alone?
3. How is sample identity checked from bedside to blood bank?

MITIGATION PRINCIPLE

Transfusion safety must never rest on a single record that one person or system can change.

DESIGN MEASURES

1. Require two independent identity checks at sampling and at the bedside, enforced by the system, not by policy alone.
2. Keep historical blood group records read-only and flag any new group that differs from them.
3. Log and alert on every manual override of electronic crossmatch or issue rules.

MAPPINGS

STRIDE	T Tampering, S Spoofing
CAPEC	CAPEC-153 Input Data Manipulation CAPEC-151 Identity Spoofing
CWE	CWE-1288 Improper Validation of Consistency within Input CWE-863 Incorrect Authorization
ATT&CK	T1565.001 Stored Data Manipulation
MDS2	IGAU Health data integrity and authenticity, AUTH Authorization, AUDT Audit controls
Standards	IEC 62304

CRI-LD-Q Outsourced pathology fails every hospital

† CARE DELAYED OR WRONG THE PATIENT · RANK Q

THREAT

Many hospitals send their tests to one shared pathology provider. When its systems are encrypted or cut off, every hospital it serves loses blood tests, crossmatching and results at once, and operations, cancer care and emergency work stop across a region.

MITIGATION PROMPTS (ON THE CARD)

1. Which hospitals stop testing if the shared provider goes down?
2. What tests can run locally when the provider is unreachable?
3. How would crossmatching continue during a regional outage?

SEEN IN PUBLIC

Synnovis pathology attack, London, 2024. Ransomware at Synnovis, pathology provider to King's College Hospital and Guy's and St Thomas', led to thousands of postponed operations and appointments and an appeal for O-type blood donors. In June 2025 King's confirmed a patient had died unexpectedly during the attack, with a long wait for a blood test result among the contributing factors; the local care board reported 170 patients harmed, mostly low harm. Sources: The Register: Qilin ransomware attack on NHS supplier contributed to patient fatality; Digital Health: Patient death linked to cyber attack on NHS pathology provider

MITIGATION PRINCIPLE

No single laboratory service should be able to stop testing for a whole region.

DESIGN MEASURES

1. Design and contract for a fallback laboratory route, with tested result and request paths, for each critical test.
2. Keep isolated, offline-capable blood bank and urgent testing capacity on each acute site.
3. Rehearse a regional pathology outage with the provider and the hospitals it serves.

MAPPINGS

STRIDE	D Denial of service
CWE	CWE-1357 Reliance on Insufficiently Trustworthy Component
ATT&CK	T1486 Data Encrypted for Impact T1199 Trusted Relationship
MDS2	DTBK Data backup and disaster recovery, CONN Connectivity capabilities
Standards	IEC 80001-1

CRI-LD-J Results stop flowing and nobody notices

† CARE DELAYED OR WRONG THE PATIENT · RANK J

THREAT

Interfaces between analysers, middleware and the record fail quietly: a stalled queue, an expired certificate, a dropped feed. Critical results sit undelivered while the ward assumes nothing abnormal came back.

MITIGATION PROMPTS (ON THE CARD)

1. How would anyone know results had stopped flowing to the record?
2. What happens to a critical result stuck in a queue?
3. Which certificates or feeds could expire silently?

MITIGATION PRINCIPLE

Silence from the laboratory must never look the same as a normal result.

DESIGN MEASURES

1. Send heartbeats on every result interface and alarm to the laboratory and IT when one stops.
2. Show pending and overdue results to the requesting clinician, with the time each was expected.
3. Phone critical results by a defined route that does not depend on the interface working.

MAPPINGS

STRIDE	D Denial of service
CWE	CWE-754 Improper Check for Unusual or Exceptional Conditions CWE-778 Insufficient Logging
ATT&CK	T1489 Service Stop
MDS2	AUDT Audit controls, CONN Connectivity capabilities
Standards	IEC 80001-1

CRI-LD-10 Autoverification rules quietly loosened

† CARE DELAYED OR WRONG THE PATIENT · RANK 10

THREAT

Laboratory systems release normal results automatically using rules, reference ranges and critical limits held in configuration. Changing those rules lets abnormal results release as normal, or suppresses critical-value calls, across every patient tested.

MITIGATION PROMPTS (ON THE CARD)

1. Who can change autoverification rules and critical limits?
2. How is a rule change reviewed before it goes live?
3. Would loosened rules be noticed across thousands of results?

MITIGATION PRINCIPLE

The rules that decide what a clinician sees must be controlled like the analyser itself.

DESIGN MEASURES

1. Put autoverification rules, reference ranges and critical limits under change control with two-person approval.
2. Compare the live rule set against an approved baseline every day and alert on any difference.
3. Sample auto-released results for manual review so a loosened rule shows up quickly.

MAPPINGS

STRIDE	T Tampering
CAPEC	CAPEC-75 Manipulating Writeable Configuration Files CAPEC-176 Configuration/Environment Manipulation
CWE	CWE-15 External Control of System or Configuration Setting CWE-732 Incorrect Permission Assignment for Critical Resource
ATT&CK	T1565.001 Stored Data Manipulation
MDS2	AUTH Authorization, AUDT Audit controls, IGAU Health data integrity and authenticity
Standards	IEC 62304

CRI-LD-9 Bedside tests filed to wrong patient

† CARE DELAYED OR WRONG THE PATIENT · RANK 9

THREAT

Glucose meters, blood gas analysers and other bedside tests rely on shared operator codes and patient barcodes that are easily bypassed. Results land on the wrong record, and the wrong patient is treated.

MITIGATION PROMPTS (ON THE CARD)

1. How is each bedside test tied to an operator and a patient?
2. Can staff bypass the patient barcode on a bedside meter?
3. Are operator codes on bedside devices individual or shared?

MITIGATION PRINCIPLE

Every bedside test must be tied to a verified operator and a verified patient.

DESIGN MEASURES

1. Require a patient wristband scan before testing, with no manual entry except a logged emergency route.
2. Give each operator an individual credential and lock devices to trained users.
3. Hold results that fail identity checks in a queue for review rather than filing them.

MAPPINGS

STRIDE	S Spoofing, R Repudiation
CAPEC	CAPEC-151 Identity Spoofing
CWE	CWE-308 Use of Single-factor Authentication CWE-1390 Weak Authentication
MDS2	PAUT Person authentication, AUTH Authorization, IGAU Health data integrity and authenticity
Standards	IEC 80001-1

CRI-LD-8 Pathology slides swapped or edited

† CARE DELAYED OR WRONG THE PATIENT · RANK 8

THREAT

Digital pathology stores whole-slide images that pathologists and AI read remotely. If images can be replaced, relabelled or edited, a cancer is missed or invented, and the error looks like a sound diagnosis.

MITIGATION PROMPTS (ON THE CARD)

1. How is a slide image bound to its specimen?
2. Who can replace or relabel stored slide images?
3. Would a pathologist see that an image had been edited?

MITIGATION PRINCIPLE

A slide image must stay bound to its specimen and provably unchanged from scanner to report.

DESIGN MEASURES

1. Hash images at the scanner and check the hash whenever an image is opened for reporting.
2. Bind each image to specimen and patient identifiers inside signed metadata, not filenames.
3. Restrict write and delete rights on the image store to the scanning workflow.

MAPPINGS

STRIDE	T Tampering, S Spoofing
CAPEC	CAPEC-148 Content Spoofing CAPEC-165 File Manipulation
CWE	CWE-353 Missing Support for Integrity Check CWE-1230 Exposure of Sensitive Information Through Metadata
ATT&CK	T1565.001 Stored Data Manipulation
MDS2	IGAU Health data integrity and authenticity, AUTH Authorization
Standards	DICOM PS3.15

CRI-LD-7 Quality control records faked

† CARE DELAYED OR WRONG THE PATIENT · RANK 7

THREAT

Quality control and calibration results show whether an analyser can be trusted. If they can be edited or skipped without trace, a drifting analyser keeps reporting wrong values and the laboratory's records say all was well.

MITIGATION PROMPTS (ON THE CARD)

1. Is quality control captured automatically or typed in?
2. Can a QC result be edited or skipped without trace?
3. Who reviews QC trends for a drifting analyser?

MITIGATION PRINCIPLE

Quality control evidence must be captured automatically and be impossible to rewrite quietly.

DESIGN MEASURES

1. Capture QC and calibration results directly from the analyser, not by manual entry.
2. Block patient result release when QC has failed or is overdue, with a logged override.
3. Keep QC history in an append-only store that analyser and laboratory staff cannot edit.

MAPPINGS

STRIDE	T Tampering, R Repudiation
CAPEC	CAPEC-268 Audit Log Manipulation
CWE	CWE-778 Insufficient Logging CWE-223 Omission of Security-relevant Information
ATT&CK	T1565.001 Stored Data Manipulation T1070 Indicator Removal
MDS2	AUDT Audit controls, IGAU Health data integrity and authenticity
Standards	IEC 62304

CRI-LD-6 Analysers as a network foothold

THE PATIENT · RANK 6

THREAT

Analysers often run an old embedded operating system that the hospital may not patch, on the same network as everything else. One compromised analyser becomes a foothold for ransomware or a route to other laboratory and clinical systems.

MITIGATION PROMPTS (ON THE CARD)

1. What can each analyser reach on the network?
2. Who patches analysers, and how long does it take?
3. What reaches the analyser that isn't its own system?

MITIGATION PRINCIPLE

An analyser should reach only what it needs and nothing should reach it except its own systems.

DESIGN MEASURES

1. Place analysers in their own network zone with allow-lists limited to middleware and vendor service.
2. Ask for an SBOM and a supported-until date before purchase, and plan replacement around it.
3. Monitor analyser traffic for anything outside its normal pattern.

MAPPINGS

STRIDE	E Elevation of privilege, T Tampering
CAPEC	CAPEC-310 Scanning for Vulnerable Software
CWE	CWE-1104 Use of Unmaintained Third Party Components CWE-1329 Reliance on Component That is Not Updateable
ATT&CK	T1210 Exploitation of Remote Services
EMB3D	TID-210 Device Vulnerabilities Unpatchable TID-202 Exploitable System Network Stack Component
MDS2	SAHD System and application hardening, MLDP Malware detection and protection, RDMP Roadmap for third-party components
Standards	IEC 80001-1 IEC 81001-5-1

CRI-LD-5 Analyser locked by reagent licensing

† CARE DELAYED OR WRONG THE PATIENT · RANK 5

THREAT

Some analysers check reagent tags or licences against the manufacturer's cloud before running. When that link fails, is blocked or the vendor is attacked, testing stops even though reagents and staff are ready.

MITIGATION PROMPTS (ON THE CARD)

1. Does testing stop if the vendor's licence service is unreachable?
2. How long can analysers run without the manufacturer's cloud?
3. Who is called when reagent checks block testing at night?

MITIGATION PRINCIPLE

Clinical testing must not depend on a vendor service being reachable at the moment of the test.

DESIGN MEASURES

1. Require offline grace periods for licence and reagent checks, written into the purchase contract.
2. Test what the analyser does when its vendor link is cut, before go-live.
3. Keep an emergency unlock procedure the laboratory can use without the vendor.

MAPPINGS

STRIDE	D Denial of service
CWE	CWE-1357 Reliance on Insufficiently Trustworthy Component
ATT&CK	T1489 Service Stop
MDS2	CONN Connectivity capabilities, RMOT Remote service
Standards	IEC 80001-1

CRI-LD-4 Genomic data leaves the building

THE PATIENT · RANK 4

THREAT

Sequencers and analysis pipelines send genomic data to cloud services. Genomes identify patients and their relatives, cannot be reissued after a breach, and are often stored with weaker controls than the clinical record.

MITIGATION PROMPTS (ON THE CARD)

1. Where do sequencers and pipelines send genomic data?
2. Are genomic data protected at least as well as the record?
3. Who could link a stored genome back to a patient's relatives?

MITIGATION PRINCIPLE

Genomic data must be treated as the most sensitive data the hospital holds.

DESIGN MEASURES

1. Encrypt genomic data at rest and in transit and keep keys under the hospital's control.
2. Separate identifiers from sequence data and link them only inside an authorised service.
3. Record every export and limit which destinations a sequencer can send data to.

MAPPINGS

STRIDE	I Information disclosure
LINDDUN	I Identifying, L Linking, DD Data disclosure
CWE	CWE-359 Exposure of Private Personal Information to an Unauthorized Actor CWE-319 Cleartext Transmission of Sensitive Information
ATT&CK	T1530 Data from Cloud Storage T1567.002 Exfiltration to Cloud Storage
MDS2	STCF Data storage confidentiality, TXCF Transmission confidentiality, DIDT Health data de-identification
Standards	ISO 27799

CRI-LD-3 Public health reports spoofed or suppressed

THE PATIENT · RANK 3

THREAT

Laboratories report notifiable infections to public health automatically. If that feed can be forged or blocked, an outbreak goes unseen, or a false one triggers costly responses and alarm.

MITIGATION PROMPTS (ON THE CARD)

1. How does public health know a notifiable report is genuine?
2. Would anyone notice the reporting feed had stopped?
3. Who checks that every required report was sent?

MITIGATION PRINCIPLE

Reports that drive public health action must be authenticated and their absence noticed.

DESIGN MEASURES

1. Authenticate both ends of the reporting link and sign each report.
2. Reconcile reported cases with laboratory positives daily and investigate gaps.
3. Alert when a reporting feed goes quiet for longer than its normal interval.

MAPPINGS

STRIDE	S Spoofing, T Tampering, D Denial of service
CAPEC	CAPEC-194 Fake the Source of Data
CWE	CWE-924 Improper Enforcement of Message Integrity During Transmission in a Communication Channel
ATT&CK	T1565.002 Transmitted Data Manipulation
MDS2	NAUT Node authentication, TXIG Transmission integrity

CRI-LD-2 Laboratory exports leak in spreadsheets

THE PATIENT · RANK 2

THREAT

Results are exported to spreadsheets for audit, research and service reviews. Identifiable data spreads into shared drives and email, and formula content in exported cells can run when the file is opened.

MITIGATION PROMPTS (ON THE CARD)

1. What identifiable data goes into exported spreadsheets?
2. Where do exported files end up, and who can open them?
3. Are exported cells checked for formula content?

MITIGATION PRINCIPLE

Data leaving the laboratory system should carry no more than the task needs.

DESIGN MEASURES

1. Pseudonymise exports by default and require approval for identifiable extracts.
2. Neutralise formula characters in exported fields.
3. Log every export with its requester, purpose and destination.

MAPPINGS

STRIDE	I Information disclosure
LINDDUN	DD Data disclosure, L Linking
CWE	CWE-1236 Improper Neutralization of Formula Elements in a CSV File CWE-212 Improper Removal of Sensitive Information Before Storage or Transfer
ATT&CK	T1005 Data from Local System
MDS2	DIDT Health data de-identification, MPII Management of private data, AUDT Audit controls
Standards	ISO 27799

CRI-CA · THE PATIENT · 13 ENTRIES

Clinical Software and AI

Software as a medical device, decision support, dose calculators, early-warning and sepsis scores, imaging AI, AI scribes and the apps clinicians reach for.

https://ostering.com/taxonomies/hospitals-and-medical-devices/clinical-software-and-ai/

CRI-CA-A Shared clinical knowledge base corrupted

† CARE DELAYED OR WRONG THE PATIENT · RANK A

THREAT

Decision support, drug interaction checks and order sets draw on a central rule base or a third-party drug database. One corrupted rule or update gives wrong advice to every prescriber at once, and the advice looks authoritative.

MITIGATION PROMPTS (ON THE CARD)

1. Who verifies changes to the clinical rule base before release?
2. How many prescribers would one corrupted rule reach?
3. How are third-party drug database updates checked?

MITIGATION PRINCIPLE

Clinical rules must be changed and updated like a medical device, with independent verification.

DESIGN MEASURES

1. Verify the signature and provenance of every knowledge base update before loading it.
2. Test each update against a fixed set of clinical cases and block it if any result changes unexpectedly.
3. Keep the previous version ready to restore and record who approved each change.

MAPPINGS

STRIDE	T Tampering
CAPEC	CAPEC-186 Malicious Software Update CAPEC-184 Software Integrity Attack
CWE	CWE-494 Download of Code Without Integrity Check CWE-684 Incorrect Provision of Specified Functionality
ATT&CK	T1565.001 Stored Data Manipulation T1195.002 Compromise Software Supply Chain
MDS2	IGAU Health data integrity and authenticity, CSUP Cybersecurity product upgrades, AUDT Audit controls
Standards	IEC 62304 ISO 14971 IEC 81001-5-1

CRI-CA-K Dose calculators trusted blindly

† CARE DELAYED OR WRONG THE PATIENT · RANK K

THREAT

Weight-based and infusion dose calculators accept whatever inputs they are given. A weight in the wrong unit, a moved decimal or a changed concentration produces a tenfold dose that looks correct on screen.

MITIGATION PROMPTS (ON THE CARD)

1. What plausibility checks does the calculator apply to its inputs?
2. Which units does each input expect, and is that shown?
3. Would a tenfold dose look any different on screen?

MITIGATION PRINCIPLE

A calculator that sets a dose must check its inputs against what is plausible for the patient.

DESIGN MEASURES

1. Take weight and concentration from verified sources, not free text, and show their origin.
2. Apply hard and soft limits by age, weight and drug, and require a reason to exceed them.
3. Show units explicitly at every step and in the final result.

MAPPINGS

STRIDE	T Tampering
CAPEC	CAPEC-153 Input Data Manipulation
CWE	CWE-1287 Improper Validation of Specified Type of Input CWE-1288 Improper Validation of Consistency within Input
MDS2	IGAU Health data integrity and authenticity
Standards	IEC 62304 ISO 14971

CRI-CA-Q Early-warning scores fed bad inputs

† CARE DELAYED OR WRONG THE PATIENT · RANK Q

THREAT

Deterioration and sepsis algorithms score whatever vital signs and results reach them. Missing, delayed or altered inputs, or a raised threshold, mean a deteriorating patient is never flagged.

MITIGATION PROMPTS (ON THE CARD)

1. How does the algorithm show that inputs are stale or missing?
2. Who can change scoring thresholds, and is it reviewed?
3. What alerts staff when an expected input never arrives?

MITIGATION PRINCIPLE

An algorithm must know when its inputs are stale, missing or implausible and say so.

DESIGN MEASURES

1. Show the age and source of every input beside the score.
2. Flag a score as incomplete when inputs are missing or late instead of treating them as normal.
3. Control and audit threshold changes, with clinical sign-off.

MAPPINGS

STRIDE	T Tampering, D Denial of service
CAPEC	CAPEC-153 Input Data Manipulation
CWE	CWE-754 Improper Check for Unusual or Exceptional Conditions CWE-1288 Improper Validation of Consistency within Input
ATT&CK	T1565.002 Transmitted Data Manipulation
MDS2	IGAU Health data integrity and authenticity, AUDT Audit controls
Standards	IEC 62304 ISO 14971

CRI-CA-J Imaging AI fooled by crafted images

† CARE DELAYED OR WRONG THE PATIENT · RANK J

THREAT

Triage and detection models read images that pass through many systems. Small, deliberate changes to an image can make a model miss a bleed or a tumour, or invent one, with no visible sign to a human reader.

MITIGATION PROMPTS (ON THE CARD)

1. Has the imaging model been tested against manipulated images?
2. Is the model ever the only reader of an image?
3. How would a missed finding by the model be caught?

MITIGATION PRINCIPLE

An imaging model must be tested against manipulated inputs and never be the only reader.

DESIGN MEASURES

1. Check image integrity from modality to model before inference.
2. Test models with adversarial and corrupted inputs during validation and after every update.
3. Keep a clinician read on every study the model triages as normal for the highest-risk findings.

MAPPINGS

STRIDE	T Tampering
CAPEC	CAPEC-153 Input Data Manipulation
CWE	CWE-1039 Inadequate Detection or Handling of Adversarial Input Perturbations in Automated Recognition Mechanism
ATT&CK	T1565.001 Stored Data Manipulation
MDS2	IGAU Health data integrity and authenticity
Standards	FDA premarket ISO 14971

CRI-CA-10 Model updates change care unannounced

† CARE DELAYED OR WRONG THE PATIENT · RANK 10

THREAT

Cloud-hosted software as a medical device can receive a new model version without the hospital knowing. Its performance on local patients shifts, and nobody compares outputs before and after.

MITIGATION PROMPTS (ON THE CARD)

1. How does the hospital learn that a model version has changed?
2. Are outputs compared on local patients before and after updates?
3. Who can pause a model whose performance has shifted?

MITIGATION PRINCIPLE

A change to a clinical model must be visible to the hospital and checked on local data.

DESIGN MEASURES

1. Require notice and release notes for every model change in the supply contract.
2. Display the model version with every output and record it in the patient record.
3. Monitor agreement and alert rates locally, and alarm on a sudden shift.

MAPPINGS

STRIDE	T Tampering, R Repudiation
CWE	CWE-1357 Reliance on Insufficiently Trustworthy Component CWE-684 Incorrect Provision of Specified Functionality
MDS2	CSUP Cybersecurity product upgrades, SGUD Security guidance
Standards	FDA premarket IEC 62304

CRI-CA-9 Automation bias hides the failure

† CARE DELAYED OR WRONG THE PATIENT · RANK 9

THREAT

Interfaces present algorithm outputs as certain, without confidence or evidence. Clinicians stop checking, so any error, drift or compromise in the software flows straight into treatment.

MITIGATION PROMPTS (ON THE CARD)

1. Does the interface show how confident the algorithm is?
2. What prompts the clinician to check an output before acting?
3. How would drift or compromise in the software become visible?

MITIGATION PRINCIPLE

Clinical software should show how sure it is and invite the clinician to check.

DESIGN MEASURES

1. Show confidence, the main inputs and known limits beside every recommendation.
2. Design workflows so the clinician records a decision, not just an acceptance.
3. Audit acceptance rates and investigate units where nearly every suggestion is accepted.

MAPPINGS

STRIDE	T Tampering
CAPEC	CAPEC-148 Content Spoofing
CWE	CWE-451 User Interface (UI) Misrepresentation of Critical Information
MDS2	IGAU Health data integrity and authenticity, SGUD Security guidance
Standards	ISO 14971

CRI-CA-8 AI scribes write errors into records

† CARE DELAYED OR WRONG THE PATIENT · RANK 8

THREAT

Ambient and speech scribes, including agent-driven tools, turn conversations into notes, allergies and medication lists. Mishearing, prompt injection from spoken or pasted text, or invented details enter the record and drive later orders.

MITIGATION PROMPTS (ON THE CARD)

1. Who checks a generated note before it enters the record?
2. Could spoken or pasted text steer what the scribe writes?
3. Which orders could be driven by an unreviewed generated entry?

MITIGATION PRINCIPLE

Nothing generated should enter the record until a clinician has checked and accepted it.

DESIGN MEASURES

1. Hold generated text as a draft that a named clinician must review and sign.
2. Highlight generated content that changes allergies, medications or diagnoses for explicit confirmation.
3. Tell patients when recording and generation are used and let them decline.

MAPPINGS

STRIDE	T Tampering, R Repudiation
LINDDUN	U Unawareness and unintervenability, DD Data disclosure
CWE	CWE-1427 Improper Neutralization of Input Used for LLM Prompting CWE-1434 Insecure Setting of Generative AI/ML Model Inference Parameters
MDS2	IGAU Health data integrity and authenticity, AUDT Audit controls, MPII Management of private data
Standards	IEC 62304 ISO 14971

CRI-CA-7 Models leak the patients they learned

THE PATIENT · RANK 7

THREAT

Models trained or fine-tuned on hospital data can reveal whether a person was in the training set, or reproduce fragments of their records, to anyone who can query them.

MITIGATION PROMPTS (ON THE CARD)

1. Could someone tell from the model whether a patient was in training?
2. Who can query the model, and how often?
3. Was the training data reduced or protected before use?

MITIGATION PRINCIPLE

Patient data used to build a model must not be recoverable from the model.

DESIGN MEASURES

1. Train on de-identified data wherever possible and test models for memorisation before release.
2. Limit who can query models and how often.
3. Record which datasets trained each model and the legal basis for using them.

MAPPINGS

STRIDE	I Information disclosure
LINDDUN	I Identifying, L Linking, DD Data disclosure, Nc Non-compliance
CWE	CWE-359 Exposure of Private Personal Information to an Unauthorized Actor
MDS2	DIDT Health data de-identification, MPII Management of private data
Standards	ISO 27799

CRI-CA-6 Unvalidated spreadsheets run clinical decisions

† CARE DELAYED OR WRONG THE PATIENT · RANK 6

THREAT

Wards and pharmacies build their own calculators, macros and trackers. They have no version control or testing, a changed cell alters every result, and macro-enabled files are an easy way to deliver malware.

MITIGATION PROMPTS (ON THE CARD)

1. Which local spreadsheets or macros inform clinical decisions?
2. Does each one have an owner, a version and a test?
3. Who could change a formula without anyone noticing?

MITIGATION PRINCIPLE

Any tool that informs a clinical decision needs an owner, a version and a test.

DESIGN MEASURES

1. Register local clinical tools, name an owner and validate them before use.
2. Lock formulas and store approved versions in a controlled location.
3. Block macros from untrusted locations on clinical workstations.

MAPPINGS

STRIDE	T Tampering, E Elevation of privilege
CAPEC	CAPEC-17 Using Malicious Files
CWE	CWE-1236 Improper Neutralization of Formula Elements in a CSV File CWE-15 External Control of System or Configuration Setting
ATT&CK	T1204.002 Malicious File
MDS2	IGAU Health data integrity and authenticity, MLDP Malware detection and protection
Standards	IEC 62304

CRI-CA-5 Consumer apps used for clinical work

THE PATIENT · RANK 5

THREAT

Staff use unregulated apps for doses, wound photos and messaging because they are quick. Patient images and details sync to personal clouds, and app results carry no validation.

MITIGATION PROMPTS (ON THE CARD)

1. Which consumer apps do staff use for clinical work, and why?
2. Where do photos and details from those apps sync?
3. Is the approved tool as quick as the app staff prefer?

MITIGATION PRINCIPLE

Make the approved tool the easiest one to use for the task.

DESIGN MEASURES

1. Provide approved apps for photos, calculations and messaging on managed devices.
2. Keep clinical photos in a managed container that never syncs to personal storage.
3. Publish which apps are approved for which clinical tasks.

MAPPINGS

STRIDE	I Information disclosure
LINDDUN	DD Data disclosure, Nc Non-compliance, U Unawareness and unintervenability
CWE	CWE-359 Exposure of Private Personal Information to an Unauthorized Actor CWE-922 Insecure Storage of Sensitive Information
ATT&CK	T1567.002 Exfiltration to Cloud Storage
MDS2	STCF Data storage confidentiality, MPII Management of private data
Standards	ISO 27799

CRI-CA-4 Cloud clinical software unreachable

† CARE DELAYED OR WRONG THE PATIENT · RANK 4

THREAT

Reporting, triage and decision software increasingly runs in a vendor's cloud. When the link, the vendor or its cloud is down, the pathway has no fallback and clinical work waits.

MITIGATION PROMPTS (ON THE CARD)

1. What happens to the pathway when the vendor's cloud is down?
2. What reduced level of service is agreed, and rehearsed?
3. How long can clinical work wait for the software to return?

MITIGATION PRINCIPLE

A clinical pathway must keep working, at a known reduced level, when its cloud software is gone.

DESIGN MEASURES

1. Define and rehearse a manual fallback for each cloud-dependent pathway.
2. Require service levels and outage notice from the vendor, and monitor availability yourself.
3. Keep essential reference data available offline.

MAPPINGS

STRIDE	D Denial of service
CWE	CWE-1357 Reliance on Insufficiently Trustworthy Component
ATT&CK	T1498 Network Denial of Service T1489 Service Stop
MDS2	CONN Connectivity capabilities, DTBK Data backup and disaster recovery
Standards	IEC 80001-1

CRI-CA-3 Alert overrides leave no trail

THE PATIENT · RANK 3

THREAT

Clinicians override drug interaction and allergy alerts many times a day. Without a recorded reason, nobody can tell a justified override from a dangerous one, or prove later what was shown.

MITIGATION PROMPTS (ON THE CARD)

1. Is a reason recorded each time a safety alert is overridden?
2. Could you later prove what alert a clinician saw?
3. Who reviews override patterns for dangerous habits?

MITIGATION PRINCIPLE

Every override of a safety alert should record who, what and why.

DESIGN MEASURES

1. Require a short coded reason for overriding high-severity alerts.
2. Record the alert text shown, with its version, alongside the override.
3. Review override patterns and retire alerts that are always overridden.

MAPPINGS

STRIDE	R Repudiation
CWE	CWE-778 Insufficient Logging CWE-223 Omission of Security-relevant Information
MDS2	AUDT Audit controls
Standards	IEC 62304

CRI-CA-2 Algorithms expose sensitive inferences

THE PATIENT · RANK 2

THREAT

Models infer pregnancy, HIV status, mental illness or addiction from routine data and show the inference to anyone viewing the patient. The patient never disclosed it and cannot see or contest it.

MITIGATION PROMPTS (ON THE CARD)

1. Which sensitive conditions can the models infer from routine data?
2. Who can see an inference the patient never disclosed?
3. Can patients see or contest what was inferred about them?

MITIGATION PRINCIPLE

Inferred sensitive information deserves the same protection as information the patient disclosed.

DESIGN MEASURES

1. Classify inferred conditions with the same sensitivity as recorded ones and restrict their display.
2. Label inferences as such and let clinicians suppress them.
3. Tell patients which inference tools are in use.

MAPPINGS

STRIDE	I Information disclosure
LINDDUN	I Identifying, DD Data disclosure, U Unawareness and unintervenability
CWE	CWE-359 Exposure of Private Personal Information to an Unauthorized Actor CWE-1220 Insufficient Granularity of Access Control
MDS2	AUTH Authorization, MPII Management of private data
Standards	ISO 27799

CRI-RC · THE HOSPITAL · 13 ENTRIES

Records and Patient Data

The EHR and patient administration, orders and results, identity matching, sensitive categories, portals, research use and the audit trail.

https://ostering.com/taxonomies/hospitals-and-medical-devices/records-and-patient-data/

CRI-RC-A Allergies and medications rewritten

† CARE DELAYED OR WRONG THE HOSPITAL · RANK A

THREAT

Clinicians act on the allergy list, medication history, blood group and resuscitation status in the record. If these can be changed without strong control and visible history, a patient is given a drug they react to, or not resuscitated.

MITIGATION PROMPTS (ON THE CARD)

1. Who can change allergies, blood group or resuscitation status?
2. How obvious is a recent change to a clinician opening the record?
3. What review follows a change to a safety-critical fact?

MITIGATION PRINCIPLE

Safety-critical facts in the record must be hard to change and every change must be obvious.

DESIGN MEASURES

1. Require re-authentication and a reason to change allergies, resuscitation status or blood group.
2. Show recent changes to safety-critical fields prominently to the next clinician.
3. Alert on bulk or unusual edits to these fields across many patients.

MAPPINGS

STRIDE	T Tampering
LINDDUN	Nc Non-compliance
CAPEC	CAPEC-1 Accessing Functionality Not Properly Constrained by ACLs
CWE	CWE-862 Missing Authorization CWE-863 Incorrect Authorization
ATT&CK	T1565.001 Stored Data Manipulation
MDS2	IGAU Health data integrity and authenticity, AUDT Audit controls, AUTH Authorization
Standards	ISO 27799

CRI-RC-K Whole record stolen for extortion

THE HOSPITAL · RANK K

THREAT

The record holds every patient's history in a few databases and reporting replicas. Attackers copy it in bulk, then extort the hospital and threaten to publish, and the data can never be taken back.

MITIGATION PROMPTS (ON THE CARD)

1. Which accounts or systems could copy the whole record?
2. Would a bulk export from a reporting replica raise an alarm?
3. How are backups and replicas protected from the same theft?

SEEN IN PUBLIC

Change Healthcare, 2024. Ransomware at Change Healthcare, which handles about one in three US health transactions, left many providers and pharmacies unable to process claims and prescriptions for weeks; the data of about 192.7 million people was taken. Sources: Becker's: Change Healthcare data breach toll reaches 192.7 million; Fierce Healthcare: UnitedHealth estimates 190M people impacted

NHS Dumfries and Galloway, 2024. A ransomware group stole data from NHS Dumfries and Galloway, claiming 3 TB, and published clinical data on patients to pressure the health board; the board said records were not altered and care continued. Sources: Help Net Security: NHS Scotland confirms ransomware attackers leaked patients' data; Digital Health: NHS Dumfries and Galloway working with NCSC after 3TB data leak

MITIGATION PRINCIPLE

No single account or system should be able to copy the whole patient record unnoticed.

DESIGN MEASURES

1. Limit bulk query and export rights to a few monitored service accounts.
2. Detect and alarm on unusual volumes leaving reporting databases and backups.
3. Encrypt replicas and backups with keys held separately from the systems that read them.

MAPPINGS

STRIDE	I Information disclosure
LINDDUN	DD Data disclosure, I Identifying
CAPEC	CAPEC-116 Excavation
CWE	CWE-359 Exposure of Private Personal Information to an Unauthorized Actor CWE-1220 Insufficient Granularity of Access Control
ATT&CK	T1213.006 Databases T1567.002 Exfiltration to Cloud Storage T1657 Financial Theft
MDS2	STCF Data storage confidentiality, AUDT Audit controls, MPII Management of private data
Standards	ISO 27799

CRI-RC-Q Patients extorted one by one

THE HOSPITAL · RANK Q

THREAT

Therapy notes, sexual health and other sensitive records are stored as readable text. Once stolen, attackers contact patients individually and demand payment to keep their notes private.

MITIGATION PROMPTS (ON THE CARD)

1. Which notes would hurt a patient most if published?
2. Are those notes stored as readable text?
3. What support would patients get if their notes were stolen?

SEEN IN PUBLIC

Vastaamo psychotherapy records, Finland, 2020. Therapy records of about 36,000 patients of the Vastaamo psychotherapy centre were stolen in 2018 and 2019; in October 2020, after the company refused to pay, patients were extorted individually. A Finnish court convicted the attacker in April 2024 and the appeal court upheld the conviction in 2025. Sources: Wikipedia: Vastaamo data breach; AP via NY1: Finnish hacker gets prison for accessing psychotherapy records

MITIGATION PRINCIPLE

The most sensitive notes must be useless to anyone who steals them.

DESIGN MEASURES

1. Encrypt sensitive note categories at field level with separately held keys.
2. Prepare a plan to warn and support patients quickly if notes are taken.
3. Keep sensitive notes out of bulk extracts and reporting copies.

MAPPINGS

STRIDE	I Information disclosure
LINDDUN	DD Data disclosure, I Identifying, L Linking
CWE	CWE-312 Cleartext Storage of Sensitive Information CWE-359 Exposure of Private Personal Information to an Unauthorized Actor
ATT&CK	T1657 Financial Theft T1005 Data from Local System
MDS2	STCF Data storage confidentiality, MPII Management of private data
Standards	ISO 27799

CRI-RC-J Two patients become one record

† CARE DELAYED OR WRONG THE HOSPITAL · RANK J

THREAT

Patient matching merges records on name, date of birth and partial identifiers. A wrong merge or a stolen identity mixes another person's allergies, results and diagnoses into a patient's record, and both are treated on the wrong history.

MITIGATION PROMPTS (ON THE CARD)

1. Which identifiers does patient matching rely on?
2. Who reviews a merge before it takes effect?
3. How is a wrong merge undone, and who is told?

MITIGATION PRINCIPLE

Merging identities must be deliberate, reviewed and reversible.

DESIGN MEASURES

1. Require review of merges below a high matching confidence, by trained staff.
2. Keep merges reversible with full history of which data came from which identity.
3. Flag records where new data conflicts with established facts, such as blood group or sex at birth.

MAPPINGS

STRIDE	S Spoofing, T Tampering
LINDDUN	L Linking, I Identifying
CAPEC	CAPEC-151 Identity Spoofing
CWE	CWE-1288 Improper Validation of Consistency within Input
MDS2	IGAU Health data integrity and authenticity, AUDT Audit controls
Standards	ISO 27799

CRI-RC-10 Sensitive categories open to every user

THE HOSPITAL · RANK 10

THREAT

Mental health, sexual health, HIV, abortion, gender identity and genetic records are visible to anyone who can open the patient. Where the law, family or employer is hostile, disclosure puts the patient at real risk.

MITIGATION PROMPTS (ON THE CARD)

1. Who can open mental health, sexual health or genetic records?
2. Does access follow the care relationship or just the login?
3. What extra step guards the most sensitive categories?

MITIGATION PRINCIPLE

Access to sensitive categories should follow the care relationship, not the login.

DESIGN MEASURES

1. Tag sensitive categories and restrict them to the treating team, with logged break-glass.
2. Let patients choose additional restrictions where the law allows.
3. Keep sensitive categories out of default printouts, summaries and shared feeds.

MAPPINGS

STRIDE	I Information disclosure
LINDDUN	DD Data disclosure, I Identifying, Nc Non-compliance
CWE	CWE-1220 Insufficient Granularity of Access Control CWE-359 Exposure of Private Personal Information to an Unauthorized Actor
MDS2	AUTH Authorization, MPII Management of private data
Standards	ISO 27799

CRI-RC-9 Staff browse records without reason

THE HOSPITAL · RANK 9

THREAT

Insiders look up celebrities, colleagues, neighbours and former partners. Access is logged, but nobody reviews the logs, so curiosity and stalking go unnoticed and unpunished.

MITIGATION PROMPTS (ON THE CARD)

1. Who reviews access logs, and how often?
2. How would a colleague browsing a neighbour's record be detected?
3. What happens to staff found looking without reason?

MITIGATION PRINCIPLE

Every look at a record should be attributable and reviewed against a care relationship.

DESIGN MEASURES

1. Analyse access logs automatically for patients with no care link to the viewer.
2. Flag high-interest records and alert on access to them.
3. Tell staff the logs are reviewed and act visibly on findings.

MAPPINGS

STRIDE	I Information disclosure, R Repudiation
LINDDUN	DD Data disclosure, D Detecting, I Identifying
CAPEC	CAPEC-122 Privilege Abuse
CWE	CWE-778 Insufficient Logging
ATT&CK	T1213 Data from Information Repositories
MDS2	AUDT Audit controls, AUTH Authorization
Standards	ISO 27799

CRI-RC-8 Patient portal accounts taken over

THE HOSPITAL · RANK 8

THREAT

Portals let patients and their proxies read records and message clinicians. Reused passwords, weak recovery and loose proxy access let attackers, or a coercive partner or relative, read and change what the patient sees.

MITIGATION PROMPTS (ON THE CARD)

1. How strong are portal logins and account recovery?
2. Who can be granted proxy access, and can the patient revoke it?
3. How would a coercive relative's access be noticed?

MITIGATION PRINCIPLE

Portal access must be as strong as the data it shows, and proxies must be revocable by the patient.

DESIGN MEASURES

1. Offer phishing-resistant authentication and detect credential stuffing.
2. Let patients see and revoke proxies, and alert them to new devices and proxy access.
3. Make account recovery require more than details found in the record.

MAPPINGS

STRIDE	S Spoofing, I Information disclosure
LINDDUN	DD Data disclosure, I Identifying, L Linking
CAPEC	CAPEC-600 Credential Stuffing
CWE	CWE-308 Use of Single-factor Authentication CWE-640 Weak Password Recovery Mechanism for Forgotten Password
ATT&CK	T1110.004 Credential Stuffing
MDS2	PAUT Person authentication, AUDT Audit controls
Standards	ISO 27799

CRI-RC-7 Health data shared beyond its purpose

THE HOSPITAL · RANK 7

THREAT

Tracking scripts on appointment and portal pages, research extracts and contracts with insurers or authorities move health data to parties the patient never expected. Once shared, it is linked with other data and cannot be recalled.

MITIGATION PROMPTS (ON THE CARD)

1. Which third parties receive data from portal and appointment pages?
2. Does every data flow have a stated purpose?
3. What does each extract contain beyond what its purpose needs?

MITIGATION PRINCIPLE

Each flow of patient data must have a stated purpose and the least data it needs.

DESIGN MEASURES

1. Remove third-party tracking from any page that shows or collects health data.
2. Keep a register of data flows with purpose, legal basis and owner, reviewed yearly.
3. Send only the fields each recipient needs.

MAPPINGS

STRIDE	I Information disclosure
LINDDUN	DD Data disclosure, U Unawareness and unintervenability, Nc Non-compliance, L Linking
CWE	CWE-201 Insertion of Sensitive Information Into Sent Data CWE-359 Exposure of Private Personal Information to an Unauthorized Actor
MDS2	MPII Management of private data, DIDT Health data de-identification
Standards	ISO 27799

CRI-RC-6 De-identified data re-identified

THE HOSPITAL · RANK 6

THREAT

Research and analytics datasets have names removed but keep dates, postcodes, rare conditions and free text. Linking them with other data identifies patients, sometimes in seconds.

MITIGATION PROMPTS (ON THE CARD)

1. Which quasi-identifiers remain in research datasets?
2. Has anyone measured the re-identification risk?
3. Who decides whether free text can leave the record?

MITIGATION PRINCIPLE

Treat de-identification as a risk to measure, not a step that is done.

DESIGN MEASURES

1. Assess re-identification risk for each release and generalise rare values.
2. Remove or scrub free text before release.
3. Release data inside a controlled research environment instead of handing out copies.

MAPPINGS

STRIDE	I Information disclosure
LINDDUN	L Linking, I Identifying, DD Data disclosure
CWE	CWE-212 Improper Removal of Sensitive Information Before Storage or Transfer CWE-359 Exposure of Private Personal Information to an Unauthorized Actor
MDS2	DIDT Health data de-identification
Standards	ISO 27799

CRI-RC-5 Audit trail can be edited

THE HOSPITAL · RANK 5

THREAT

System administrators and vendor support can change or delete audit records. Then nobody can prove who changed a record or viewed it, which matters in incidents, complaints and court.

MITIGATION PROMPTS (ON THE CARD)

1. Who can alter or delete audit records, including vendor support?
2. Where is the audit trail kept, out of administrators' reach?
3. Could you prove in court who viewed a record?

MITIGATION PRINCIPLE

The audit trail must be beyond the reach of the people and systems it records.

DESIGN MEASURES

1. Ship audit records to a separate, append-only store as they are written.
2. Separate audit administration from system administration.
3. Check the audit stream for gaps and alarm when it stops.

MAPPINGS

STRIDE	R Repudiation
LINDDUN	Nr Non-repudiation
CAPEC	CAPEC-268 Audit Log Manipulation
CWE	CWE-778 Insufficient Logging CWE-223 Omission of Security-relevant Information
ATT&CK	T1070 Indicator Removal
MDS2	AUDT Audit controls
Standards	ISO 27799

CRI-RC-4 Records released to impostors

THE HOSPITAL · RANK 4

THREAT

Records teams answer requests from patients, police, insurers and solicitors by phone, email and post. Someone posing as the patient or an official obtains a full record.

MITIGATION PROMPTS (ON THE CARD)

1. How do records staff verify who is asking for a record?
2. Which requests arrive by phone or email, and how are they checked?
3. What would an impostor need to obtain a full record?

MITIGATION PRINCIPLE

Release of records must verify who is asking and whether they are entitled.

DESIGN MEASURES

1. Verify identity through a channel already on file, not one given in the request.
2. Send records through an authenticated portal rather than email or post.
3. Review third-party requests for entitlement and release the minimum needed.

MAPPINGS

STRIDE	S Spoofing, I Information disclosure
LINDDUN	DD Data disclosure, I Identifying
CAPEC	CAPEC-407 Pretexting CAPEC-412 Pretexting via Customer Service
CWE	CWE-1390 Weak Authentication
ATT&CK	T1598.004 Spearphishing Voice
MDS2	PAUT Person authentication, MPII Management of private data
Standards	ISO 27799

CRI-RC-3 Printouts and caches left behind

THE HOSPITAL · RANK 3

THREAT

Shared workstations, browser caches, downloaded letters and downtime printouts hold patient data long after the task. Anyone using the next session, bin or printer tray can read them.

MITIGATION PROMPTS (ON THE CARD)

1. What patient data stays on shared workstations after a session?
2. Where do downtime printouts end up?
3. Who clears browser caches and downloaded letters, and when?

MITIGATION PRINCIPLE

Patient data should not outlive the task on shared equipment.

DESIGN MEASURES

1. Clear local caches and downloads when a clinical session ends.
2. Use secure print release and confidential waste on wards.
3. Lock or log off unattended sessions quickly, using tap-to-switch to keep it practical.

MAPPINGS

STRIDE	I Information disclosure
LINDDUN	DD Data disclosure
CAPEC	CAPEC-204 Lifting Sensitive Data Embedded in Cache
CWE	CWE-524 Use of Cache Containing Sensitive Information CWE-525 Use of Web Browser Cache Containing Sensitive Information
ATT&CK	T1005 Data from Local System
MDS2	ALOF Automatic logoff, STCF Data storage confidentiality
Standards	ISO 27799

CRI-RC-2 Patients cannot see who looked

THE HOSPITAL · RANK 2

THREAT

Patients have no view of who accessed their record or where it was shared. They cannot notice misuse, object to a disclosure or correct what was sent.

MITIGATION PROMPTS (ON THE CARD)

1. Can patients see who accessed their record?
2. How would a patient object to a disclosure?
3. Where can patients see where their record was shared?

MITIGATION PRINCIPLE

Patients should be able to see how their record has been used.

DESIGN MEASURES

1. Show patients an access and sharing history in the portal.
2. Let patients report access they do not recognise and track the response.
3. Explain in plain language who routinely sees their record and why.

MAPPINGS

STRIDE	R Repudiation
LINDDUN	U Unawareness and unintervenability, Nc Non-compliance
CWE	CWE-223 Omission of Security-relevant Information
MDS2	AUDT Audit controls, MPII Management of private data
Standards	ISO 27799

CRI-IN · THE HOSPITAL · 13 ENTRIES

Integration and Interoperability

HL7 v2, FHIR, DICOM, integration engines, device integration middleware and regional exchange.

https://ostering.com/taxonomies/hospitals-and-medical-devices/integration-and-interoperability/

CRI-IN-A Unauthenticated orders and results feeds

† CARE DELAYED OR WRONG THE HOSPITAL · RANK A

THREAT

Interfaces accept HL7 orders, results and admissions from any sender that can reach the port, with no check of who sent them. A forged potassium result or a cancelled allergy lands in the record looking genuine, and clinicians treat the patient on it.

MITIGATION PROMPTS (ON THE CARD)

1. Which senders can reach each interface port?
2. How does an interface check who sent a message?
3. What would a forged result look like when it reached the record?

MITIGATION PRINCIPLE

Every interface accepts clinical messages only from authenticated senders over protected channels, and rejects everything else.

DESIGN MEASURES

1. Wrap HL7 v2 MLLP feeds in mutually authenticated TLS, or carry them over an authenticated tunnel between named endpoints.
2. Allowlist sending applications and facilities per interface, and reject messages whose sender fields do not match the authenticated peer.
3. Alert on messages from unexpected sources, and route clinically significant result changes for human review.

MAPPINGS

STRIDE	S Spoofing, T Tampering
CAPEC	CAPEC-151 Identity Spoofing CAPEC-148 Content Spoofing CAPEC-594 Traffic Injection
CWE	CWE-306 Missing Authentication for Critical Functionality CWE-940 Improper Verification of Source of a Communication Channel CWE-346 Origin Validation Error
ATT&CK	T1565.002 Transmitted Data Manipulation T1557 Adversary-in-the-Middle
MDS2	NAUT Node authentication, TXIG Transmission integrity, IGAU Health data integrity and authenticity
Standards	IEC 80001-1 IEC 81001-5-1

CRI-IN-K Integration engine as master key

† CARE DELAYED OR WRONG THE HOSPITAL · RANK K

THREAT

The integration engine sees, transforms and routes every clinical message, and its routes can be edited by a handful of accounts. Whoever controls it can rewrite results, redirect orders or copy every message out, across every connected system at once.

MITIGATION PROMPTS (ON THE CARD)

1. Who can edit routes and transforms in the integration engine?
2. How are engine changes reviewed and detected?
3. What could someone controlling the engine change across systems?

MITIGATION PRINCIPLE

The integration engine is treated as a safety-critical system: changes to routes and transforms are controlled, reviewed and detectable.

DESIGN MEASURES

1. Put route and transform changes through change control with two-person approval and versioned, signed configuration.
2. Separate engine administration from ordinary IT accounts, with phishing-resistant MFA and a dedicated management network.
3. Reconcile message counts and checksums between sending and receiving systems so silent rewrites show up.
4. Keep a tested standby engine and a documented manual workaround for each critical feed.

MAPPINGS

STRIDE	T Tampering, I Information disclosure, D Denial of service, E Elevation of privilege
LINDDUN	DD Data disclosure
CAPEC	CAPEC-385 Transaction or Event Tampering via Application API Manipulation CAPEC-176 Configuration/Environment Manipulation
CWE	CWE-732 Incorrect Permission Assignment for Critical Resource CWE-1220 Insufficient Granularity of Access Control
ATT&CK	T1565.002 Transmitted Data Manipulation T1119 Automated Collection
MDS2	AUTH Authorization, AUDT Audit controls, IGAU Health data integrity and authenticity
Standards	IEC 80001-1

CRI-IN-Q Device data charted without integrity

† CARE DELAYED OR WRONG THE HOSPITAL · RANK Q

THREAT

Device integration middleware writes vital signs, pump rates and ventilator settings into the record without proving which device produced them or that values were not changed in transit. Wrong values become the charted truth that drives early-warning scores and treatment decisions.

MITIGATION PROMPTS (ON THE CARD)

1. How does middleware prove which device produced a value?
2. What validation happens before device data is charted?
3. Which scores and decisions consume charted device data?

MITIGATION PRINCIPLE

Device data entering the record carries proof of its source and integrity, and is validated before it is charted.

DESIGN MEASURES

1. Authenticate each device to the middleware and sign or MAC observations end to end, not only per network hop.
2. Require clinician validation of device data before charting, with the device identifier shown alongside each value.
3. Range-check and rate-check incoming values against physiology and the device's own reported limits.

MAPPINGS

STRIDE	S Spoofing, T Tampering, R Repudiation
CAPEC	CAPEC-384 Application API Message Manipulation via Man-in-the-Middle CAPEC-194 Fake the Source of Data
CWE	CWE-924 Improper Enforcement of Message Integrity During Transmission in a Communication Channel CWE-353 Missing Support for Integrity Check CWE-940 Improper Verification of Source of a Communication Channel
ATT&CK	T1565.002 Transmitted Data Manipulation
EMB3D	TID-406 Unauthorized Messages or Connections TID-407 Missing Message Replay Protection
MDS2	IGAU Health data integrity and authenticity, NAUT Node authentication, TXIG Transmission integrity
Standards	IEC 80001-1 IEC TR 60601-4-5

CRI-IN-J Open DICOM nodes

† CARE DELAYED OR WRONG THE HOSPITAL · RANK J

THREAT

Imaging systems accept DICOM store, query and retrieve requests from any node that knows an application title, which is usually guessable. Images can be pulled out in bulk, or new images inserted into a patient's study, including files that also carry executable code.

MITIGATION PROMPTS (ON THE CARD)

1. Which nodes can query or store to the imaging systems?
2. Is any DICOM peer authenticated beyond its application title?
3. How are received objects checked before joining a study?

SEEN IN PUBLIC

Open PACS servers, 2019. Greenbone found about 590 imaging archive (PACS) servers reachable on the internet without protection, exposing records of about 24 million patients and hundreds of millions of images; an update later counted over a billion images. Sources: Help Net Security: Confidential data of 24.3 million patients discovered online; HIPAA Journal: Exposed medical image total rises to 1.19 billion

DICOM files carrying malware, 2019. Cylera researchers showed that the DICOM file format allows an image file to also be a working Windows executable, so malware could hide inside medical images protected as patient data (CVE-2019-11687). Sources: NVD: CVE-2019-11687; GovInfoSecurity: Researchers, malware can be hidden in medical images

MITIGATION PRINCIPLE

DICOM associations are authenticated and limited to known peers, and every received object is checked before it reaches a study.

DESIGN MEASURES

1. Use DICOM TLS with certificates per node, and restrict associations to an allowlist of application titles and addresses.
2. Never expose PACS or modality DICOM ports to the internet; reach remote sites through authenticated gateways.
3. Scan received DICOM files for embedded executable content and quarantine objects arriving from unexpected sources.

MAPPINGS

STRIDE	S Spoofing, T Tampering, I Information disclosure
LINDDUN	DD Data disclosure, I Identifying
CAPEC	CAPEC-151 Identity Spoofing CAPEC-636 Hiding Malicious Data or Code within Files CAPEC-157 Sniffing Attacks
CWE	CWE-306 Missing Authentication for Critical Functionality CWE-923 Improper Restriction of Communication Channel to Intended Endpoints CWE-434 Unrestricted Upload of File with Dangerous Type
ATT&CK	T1190 Exploit Public-Facing Application T1565.001 Stored Data Manipulation
MDS2	NAUT Node authentication, TXCF Transmission confidentiality, MLDP Malware detection and protection
Standards	DICOM PS3.15 IEC 80001-1

CRI-IN-10 Identity mismatched across interfaces

† CARE DELAYED OR WRONG THE HOSPITAL · RANK 10

THREAT

Each system keys patients differently and interfaces map identifiers with brittle rules. A mapping error, or a deliberate edit to a demographic message, merges two people or files results under the wrong patient, so treatment follows someone else's data.

MITIGATION PROMPTS (ON THE CARD)

1. Which identifiers do interfaces use to match a patient?
2. Who reviews mismatches flagged between systems?
3. How would results filed to the wrong patient be noticed?

MITIGATION PRINCIPLE

Patient identity is matched on multiple strong identifiers end to end, and every merge or mismatch is detected and reviewed.

DESIGN MEASURES

1. Use an enterprise master patient index and match on at least two independent identifiers in every interface.
2. Hold and queue messages whose identifiers fail to match rather than guessing, and alert the owning team.
3. Log and review every patient merge and unmerge, with the ability to trace and reverse filed results.

MAPPINGS

STRIDE	T Tampering, R Repudiation
LINDDUN	L Linking, I Identifying
CAPEC	CAPEC-153 Input Data Manipulation
CWE	CWE-694 Use of Multiple Resources with Duplicate Identifier CWE-706 Use of Incorrectly-Resolved Name or Reference
ATT&CK	T1565.002 Transmitted Data Manipulation
MDS2	IGAU Health data integrity and authenticity, AUDT Audit controls
Standards	IEC 80001-1

CRI-IN-9 Over-broad scopes for FHIR apps

THE HOSPITAL · RANK 9

THREAT

Third-party and patient-facing apps get FHIR access through broad scopes or long-lived tokens granted once. A compromised or careless app can read whole populations' records through a legitimate API, and nobody notices because the calls look normal.

MITIGATION PROMPTS (ON THE CARD)

1. What scopes and token lifetimes do FHIR apps receive?
2. Who approves a new app's access, and for what purpose?
3. Would bulk reads through a legitimate API raise an alert?

MITIGATION PRINCIPLE

API access is granted per purpose, minimal in scope and time, and monitored for unusual volume.

DESIGN MEASURES

1. Grant the narrowest SMART scopes needed, prefer patient-level over system-level access, and expire refresh tokens.
2. Rate-limit and alert on bulk queries and access patterns outside an app's declared purpose.
3. Review registered apps regularly and revoke those without an owner or current agreement.

MAPPINGS

STRIDE	I Information disclosure, E Elevation of privilege
LINDDUN	DD Data disclosure, U Unawareness and unintervenability, Nc Non-compliance
CAPEC	CAPEC-1 Accessing Functionality Not Properly Constrained by ACLs CAPEC-57 Utilizing REST's Trust in the System Resource to Obtain Sensitive Data
CWE	CWE-1220 Insufficient Granularity of Access Control CWE-863 Incorrect Authorization CWE-770 Allocation of Resources Without Limits or Throttling
ATT&CK	T1213 Data from Information Repositories T1567 Exfiltration Over Web Service
MDS2	AUTH Authorization, MPII Management of private data, AUDT Audit controls
Standards	ISO 27799

CRI-IN-8 Replayed and duplicated messages

† CARE DELAYED OR WRONG THE HOSPITAL · RANK 8

THREAT

Interfaces cannot tell a new message from a resent one. A replayed medication order, admission or transfer is acted on twice: a second dose dispensed, a bed reassigned, a discharge triggered.

MITIGATION PROMPTS (ON THE CARD)

1. How does each interface recognise a duplicated message?
2. Which repeated messages could cause harm if acted on twice?
3. Where are message order and uniqueness enforced?

MITIGATION PRINCIPLE

Every clinical message is unique, ordered and processed once, and duplicates are caught before they act.

DESIGN MEASURES

1. Enforce unique message control IDs with sequence checking and reject duplicates within a defined window.
2. Make order processing idempotent so a resent order updates rather than duplicates.
3. Timestamp and sign messages so stale replays outside their validity window are refused.

MAPPINGS

STRIDE	T Tampering, R Repudiation
CAPEC	CAPEC-60 Reusing Session IDs (aka Session Replay) CAPEC-594 Traffic Injection
CWE	CWE-294 Authentication Bypass by Capture-replay CWE-924 Improper Enforcement of Message Integrity During Transmission in a Communication Channel
ATT&CK	T1565.002 Transmitted Data Manipulation
EMB3D	TID-221 Authentication Bypass By Message Replay TID-407 Missing Message Replay Protection
MDS2	TXIG Transmission integrity, IGAU Health data integrity and authenticity

CRI-IN-7 Feeds that fail silently

† CARE DELAYED OR WRONG THE HOSPITAL · RANK 7

THREAT

When an interface stops, queues fill quietly and the receiving system simply shows nothing new. Critical results, allergy updates or admissions stop arriving, and clinicians take the silence for normal.

MITIGATION PROMPTS (ON THE CARD)

1. How would anyone know a critical feed had stopped?
2. Who is told when interface queues back up?
3. What do clinicians see when no new data arrives?

MITIGATION PRINCIPLE

Every critical feed is monitored end to end, and staff are told when data stops flowing.

DESIGN MEASURES

1. Monitor queue depth and message age per critical feed, with alerts to an owner who is on duty around the clock.
2. Send heartbeat messages and show a visible stale-data warning in receiving systems when they stop.
3. Define and rehearse what wards do when a feed is down, including phoning critical results.

MAPPINGS

STRIDE	D Denial of service
CAPEC	CAPEC-603 Blockage
CWE	CWE-392 Missing Report of Error Condition CWE-778 Insufficient Logging
ATT&CK	T1489 Service Stop
MDS2	DTBK Data backup and disaster recovery, AUDT Audit controls
Standards	IEC 80001-1

CRI-IN-6 Exchange trusts every participant equally

THE HOSPITAL · RANK 6

THREAT

Regional and national record exchanges give every connected organisation the same reach. One compromised clinic, vendor or pharmacy can query or push records about patients it has never treated.

MITIGATION PROMPTS (ON THE CARD)

1. What can one participant query through the exchange?
2. Is access tied to a care relationship with the patient?
3. Who monitors each organisation's use of the exchange?

MITIGATION PRINCIPLE

Access through exchanges is tied to a demonstrated care relationship, and each participant's use is monitored.

DESIGN MEASURES

1. Require a care-relationship or consent assertion per query and audit it against later activity.
2. Apply per-participant quotas and anomaly detection, and suspend participants quickly when misuse shows.
3. Sign pushed documents at source so receivers can check provenance before filing them.

MAPPINGS

STRIDE	S Spoofing, I Information disclosure, E Elevation of privilege
LINDDUN	DD Data disclosure, L Linking, Nc Non-compliance
CAPEC	CAPEC-21 Exploitation of Trusted Identifiers CAPEC-122 Privilege Abuse
CWE	CWE-863 Incorrect Authorization CWE-346 Origin Validation Error
ATT&CK	T1199 Trusted Relationship T1213 Data from Information Repositories
MDS2	AUTH Authorization, AUDT Audit controls, NAUT Node authentication
Standards	ISO 27799

CRI-IN-5 Malformed messages break the engine

THE HOSPITAL · RANK 5

THREAT

Parsers in engines and receiving systems trust message structure. Oversized fields, unexpected segments or crafted XML and JSON crash interfaces, inject content downstream, or exhaust resources, stopping clinical data flows hospital-wide.

MITIGATION PROMPTS (ON THE CARD)

1. Does every interface validate messages against a strict profile?
2. What happens to a malformed or oversized message?
3. Could one bad message stop data flows hospital-wide?

MITIGATION PRINCIPLE

Every interface validates structure and content against a strict profile before processing.

DESIGN MEASURES

1. Validate messages against conformance profiles and reject or quarantine anything outside them.
2. Disable external entity resolution and limit message size, nesting and field length in all parsers.
3. Fuzz test interfaces before go-live and after upgrades.

MAPPINGS

STRIDE	T Tampering, D Denial of service
CAPEC	CAPEC-28 Fuzzing CAPEC-221 Data Serialization External Entities Blowup CAPEC-153 Input Data Manipulation
CWE	CWE-611 Improper Restriction of XML External Entity Reference CWE-776 Improper Restriction of Recursive Entity References in DTDs CWE-1284 Improper Validation of Specified Quantity in Input
ATT&CK	T1499 Endpoint Denial of Service
MDS2	SAHD System and application hardening, IGAU Health data integrity and authenticity
Standards	IEC 81001-5-1

CRI-IN-4 Shared interface credentials and certificates

THE HOSPITAL · RANK 4

THREAT

Interface accounts, keys and certificates are hard-coded, shared across feeds and vendors, and tracked nowhere. One leaked secret opens many interfaces, and an expiring certificate stops several feeds at once without warning.

MITIGATION PROMPTS (ON THE CARD)

1. Which interface credentials are shared across feeds or vendors?
2. Who owns each certificate, and who watches its expiry?
3. How many interfaces would one leaked secret open?

MITIGATION PRINCIPLE

Each interface has its own managed credentials, with known owners, rotation and expiry monitoring.

DESIGN MEASURES

1. Issue a distinct credential or certificate per interface and peer, stored in a secrets manager rather than config files.
2. Track expiry dates centrally and alert well before any certificate lapses.
3. Rotate interface secrets on schedule and whenever a vendor engineer or integrator leaves.

MAPPINGS

STRIDE	S Spoofing, D Denial of service
CAPEC	CAPEC-560 Use of Known Domain Credentials
CWE	CWE-798 Use of Hard-coded Credentials CWE-298 Improper Validation of Certificate Expiration CWE-522 Insufficiently Protected Credentials
ATT&CK	T1552.001 Credentials In Files T1078 Valid Accounts
MDS2	NAUT Node authentication, SGUD Security guidance

CRI-IN-3 Test interfaces wired to production

THE HOSPITAL · RANK 3

THREAT

Test and training systems are connected to live feeds for convenience. Test orders and dummy results flow into real records, or copies of real patient data sit in test systems with weaker controls.

MITIGATION PROMPTS (ON THE CARD)

1. Are any test or training systems connected to live feeds?
2. Where could test orders reach a real patient's record?
3. What real patient data sits in test environments?

MITIGATION PRINCIPLE

Test and live environments are separated, and only synthetic or de-identified data crosses into test.

DESIGN MEASURES

1. Block network routes between test and production interfaces, and use distinct identifiers that live systems reject.
2. Use synthetic or de-identified data in test, and approve any exception formally with an expiry date.
3. Mark test messages clearly and alert if one ever arrives in production.

MAPPINGS

STRIDE	T Tampering, I Information disclosure
LINDDUN	DD Data disclosure, Nc Non-compliance
CAPEC	CAPEC-176 Configuration/Environment Manipulation
CWE	CWE-1269 Product Released in Non-Release Configuration
MDS2	DIDT Health data de-identification, SAHD System and application hardening
Standards	IEC 80001-1

CRI-IN-2 Patient data in interface logs

THE HOSPITAL · RANK 2

THREAT

Engines keep full messages in logs, error queues and debug traces for troubleshooting, often for years. Support staff, vendors and anyone with log access can read complete patient records outside the controls of the clinical system.

MITIGATION PROMPTS (ON THE CARD)

1. How much patient data do engine logs and error queues keep?
2. Who can read interface logs, including vendors?
3. How long are full messages retained for troubleshooting?

MITIGATION PRINCIPLE

Interface logs keep only what troubleshooting needs, for as short a time as possible, under the same protection as the record.

DESIGN MEASURES

1. Mask or truncate patient identifiers and clinical content in logs by default.
2. Encrypt error queues and set retention limits that purge resolved messages.
3. Restrict and audit access to logs, including vendor support access.

MAPPINGS

STRIDE	I Information disclosure
LINDDUN	DD Data disclosure, U Unawareness and unintervenability, Nc Non-compliance
CAPEC	CAPEC-497 File Discovery
CWE	CWE-532 Insertion of Sensitive Information into Log File CWE-312 Cleartext Storage of Sensitive Information
ATT&CK	T1005 Data from Local System
MDS2	MPII Management of private data, STCF Data storage confidentiality, AUDT Audit controls
Standards	ISO 27799

CRI-NW · THE HOSPITAL · 13 ENTRIES

Networks and Wireless

Segmentation, legacy systems inside devices, Wi-Fi, WMTS telemetry, Bluetooth, RTLS, device inventory and satellite sites.

https://ostering.com/taxonomies/hospitals-and-medical-devices/networks-and-wireless/

CRI-NW-A Life support on the office network

† DIRECT HARM THE HOSPITAL · RANK A

THREAT

Monitors, pumps, ventilators and imaging share flat network segments with office PCs and email. Ransomware or a worm landing on one desktop spreads to clinical devices, which stop or must be pulled off the network mid-care.

MITIGATION PROMPTS (ON THE CARD)

1. Which clinical devices share a segment with office PCs?
2. What flows does each clinical segment actually need?
3. How would ransomware on one desktop reach a ventilator?

SEEN IN PUBLIC

WannaCry and the NHS, 2017. WannaCry ransomware disrupted at least 81 of England's 236 NHS trusts and infected 595 GP practices; the NAO estimated over 19,000 appointments were cancelled, and some trusts diverted ambulances. Sources: NAO: Investigation, WannaCry cyber attack and the NHS; GOV.UK: Foreign Office Minister condemns North Korean actor for WannaCry attacks

MITIGATION PRINCIPLE

Clinical devices sit in segments sized to their safety role, with only the flows they need allowed.

DESIGN MEASURES

1. Segment medical devices by function and criticality, and permit only documented flows to named systems.
2. Block office-to-device traffic by default, including file sharing and remote desktop protocols.
3. Design devices to keep delivering therapy and local alarms when network segments are isolated in an incident.

MAPPINGS

STRIDE	T Tampering, D Denial of service, E Elevation of privilege
CAPEC	CAPEC-700 Network Boundary Bridging
CWE	CWE-653 Improper Isolation or Compartmentalization CWE-923 Improper Restriction of Communication Channel to Intended Endpoints
ATT&CK	T1210 Exploitation of Remote Services T0866 Exploitation of Remote Services
MDS2	CONN Connectivity capabilities, SAHD System and application hardening
Standards	IEC 80001-1 IEC 62443

CRI-NW-K Unpatchable systems inside devices

† CARE DELAYED OR WRONG THE HOSPITAL · RANK K

THREAT

Imaging, lab and monitoring devices run frozen, certified builds of old operating systems that cannot be patched or run endpoint protection without the manufacturer. Known, public exploits reach them as soon as anything else on their network is compromised.

MITIGATION PROMPTS (ON THE CARD)

1. Which devices run operating systems that cannot be patched?
2. What network controls compensate for each unpatchable device?
3. When is each one due to be replaced?

SEEN IN PUBLIC

WannaCry and the NHS, 2017. WannaCry ransomware disrupted at least 81 of England's 236 NHS trusts and infected 595 GP practices; the NAO estimated over 19,000 appointments were cancelled, and some trusts diverted ambulances. Sources: NAO: Investigation, WannaCry cyber attack and the NHS; GOV.UK: Foreign Office Minister condemns North Korean actor for WannaCry attacks

MITIGATION PRINCIPLE

Devices that cannot be patched are compensated for by the network around them, and replaced on a planned date.

DESIGN MEASURES

1. Place unpatchable devices behind dedicated enforcement points that allow only their documented protocols.
2. Require manufacturers to state patch support periods and validated update timelines at procurement.
3. Monitor these segments for exploit traffic and keep a replacement date on every device record.

MAPPINGS

STRIDE	T Tampering, D Denial of service, E Elevation of privilege
CAPEC	CAPEC-310 Scanning for Vulnerable Software
CWE	CWE-1104 Use of Unmaintained Third Party Components CWE-1329 Reliance on Component That is Not Updateable
ATT&CK	T1210 Exploitation of Remote Services
EMB3D	TID-210 Device Vulnerabilities Unpatchable
MDS2	CSUP Cybersecurity product upgrades, RDMP Roadmap for third-party components, MLDP Malware detection and protection
Standards	IEC 80001-1 AAMI SW96

CRI-NW-Q Telemetry lost without an alarm

† CARE DELAYED OR WRONG THE HOSPITAL · RANK Q

THREAT

Wireless telemetry and Wi-Fi monitors drop out when the spectrum is jammed, crowded or misconfigured. Ambulatory and cardiac patients go unmonitored while the central station shows stale or missing traces that nobody treats as an alarm.

MITIGATION PROMPTS (ON THE CARD)

1. Where on site is wireless monitoring coverage weak?
2. What raises an alarm when a wireless link drops?
3. Who watches the spectrum used by telemetry?

MITIGATION PRINCIPLE

Loss of a wireless monitoring link is itself an alarm, raised locally and centrally.

DESIGN MEASURES

1. Raise a technical alarm at the bedside and central station whenever a wireless link drops beyond a short threshold.
2. Survey and manage the spectrum for telemetry bands and clinical Wi-Fi, with interference monitoring in ward areas.
3. Define which patients cannot be on wireless-only monitoring and plan fallback to wired or observation.

MAPPINGS

STRIDE	D Denial of service
CAPEC	CAPEC-601 Jamming CAPEC-604 Wi-Fi Jamming
CWE	CWE-754 Improper Check for Unusual or Exceptional Conditions
ATT&CK	T0815 Denial of View T0829 Loss of View
MDS2	CONN Connectivity capabilities
Standards	IEC 80001-1 IEC TR 60601-4-5

CRI-NW-J Clinical systems reachable from the internet

THE HOSPITAL · RANK J

THREAT

PACS, device consoles and vendor service ports end up reachable from the internet through misconfigured firewalls, NAT rules or vendor cellular modems. Search engines index them, and anyone can find patient images or a way in.

MITIGATION PROMPTS (ON THE CARD)

1. Which clinical systems could be found from the internet today?
2. Which vendor modems bypass the hospital firewall?
3. When was external exposure last checked, and by whom?

SEEN IN PUBLIC

Open PACS servers, 2019. Greenbone found about 590 imaging archive (PACS) servers reachable on the internet without protection, exposing records of about 24 million patients and hundreds of millions of images; an update later counted over a billion images. Sources: Help Net Security: Confidential data of 24.3 million patients discovered online; HIPAA Journal: Exposed medical image total rises to 1.19 billion

MITIGATION PRINCIPLE

No clinical system is reachable from the internet except through an authenticated, monitored gateway.

DESIGN MEASURES

1. Scan the hospital's own address ranges from outside regularly and act on any clinical service found.
2. Ban direct internet exposure of devices and route vendor access through a managed remote-access gateway.
3. Inventory cellular modems and out-of-band links built into devices and close or monitor them.

MAPPINGS

STRIDE	I Information disclosure, E Elevation of privilege
LINDDUN	DD Data disclosure
CAPEC	CAPEC-292 Host Discovery CAPEC-300 Port Scanning
CWE	CWE-1188 Initialization of a Resource with an Insecure Default CWE-923 Improper Restriction of Communication Channel to Intended Endpoints
ATT&CK	T1190 Exploit Public-Facing Application T1133 External Remote Services
EMB3D	TID-310 Remotely Accessible Unauthenticated Services
MDS2	CONN Connectivity capabilities, RMOT Remote service
Standards	IEC 80001-1

CRI-NW-10 Shared network stack flaws

† DIRECT HARM THE HOSPITAL · RANK 10

THREAT

Many device types embed the same third-party network stack. One flaw in it lets a single malformed packet crash or take over pumps, monitors and imaging from many makers, and nobody knows which devices carry it.

MITIGATION PROMPTS (ON THE CARD)

1. Which devices embed the same third-party network stack?
2. How quickly could affected devices be shielded on the network?
3. Where would you learn about a flaw in that stack?

SEEN IN PUBLIC

URGENT/11, 2019. The FDA warned that 11 vulnerabilities in IPnet, a third-party network stack inside several embedded operating systems, could let attackers take over or crash medical devices and hospital network equipment, and that manufacturers might not know their products contained it. Sources: Healthcare IT News: URGENT/11, FDA issues alert

MITIGATION PRINCIPLE

The hospital knows which components each device contains and can shield affected devices quickly.

DESIGN MEASURES

1. Require SBOMs at procurement and map them against the device inventory so stack flaws resolve to device lists.
2. Keep network signatures and filtering ready to shield vulnerable device segments within hours.
3. Require manufacturers to fuzz their network stacks and disclose affected models promptly.

MAPPINGS

STRIDE	D Denial of service, E Elevation of privilege
CAPEC	CAPEC-28 Fuzzing
CWE	CWE-1395 Dependency on Vulnerable Third-Party Component CWE-1104 Use of Unmaintained Third Party Components
ATT&CK	T1210 Exploitation of Remote Services T0814 Denial of Service
EMB3D	TID-202 Exploitable System Network Stack Component TID-405 Network Stack Resource Exhaustion
MDS2	SBOM Software bill of materials, CSUP Cybersecurity product upgrades, RDMP Roadmap for third-party components
Standards	AAMI SW96 FDA premarket

CRI-NW-9 Spoofed and shared Wi-Fi

THE HOSPITAL · RANK 9

THREAT

Medical devices join clinical Wi-Fi with one pre-shared key that never changes and is printed in service manuals. Anyone with the key can join, impersonate the network with an evil twin, or read and alter device traffic.

MITIGATION PROMPTS (ON THE CARD)

1. How do devices authenticate to clinical Wi-Fi?
2. When did the pre-shared key last change, and who knows it?
3. How would devices detect an evil twin network?

MITIGATION PRINCIPLE

Devices authenticate to the network individually, and the network authenticates itself to devices.

DESIGN MEASURES

1. Use certificate-based 802.1X for devices that support it, and per-device keys for those that do not.
2. Detect rogue and evil-twin access points in clinical areas and contain them.
3. Rotate any shared keys on staff and vendor departures and remove them from documentation.

MAPPINGS

STRIDE	S Spoofing, I Information disclosure, T Tampering
LINDDUN	DD Data disclosure
CAPEC	CAPEC-94 Adversary in the Middle (AiTM) CAPEC-616 Establish Rogue Location
CWE	CWE-1391 Use of Weak Credentials CWE-322 Key Exchange without Entity Authentication
ATT&CK	T1557.004 Evil Twin T0860 Wireless Compromise
EMB3D	TID-411 Weak/Insecure Cryptographic Protocol
MDS2	NAUT Node authentication, TXCF Transmission confidentiality
Standards	IEC 80001-1

CRI-NW-8 No list of connected devices

THE HOSPITAL · RANK 8

THREAT

Nobody can say which medical devices are on the network, where they are, what software they run or who owns them. Segmentation, patching, incident response and recalls all start by guessing.

MITIGATION PROMPTS (ON THE CARD)

1. Can you list every connected device, its location and owner?
2. How is the inventory kept current as devices move?
3. How long would a recall search take today?

MITIGATION PRINCIPLE

Every connected device is known, with its location, software, owner and risk recorded and kept current.

DESIGN MEASURES

1. Combine passive network discovery with the clinical engineering asset register and reconcile them continuously.
2. Record software versions, SBOM, network flows and clinical criticality for every connected device.
3. Make network connection depend on the device being registered.

MAPPINGS

STRIDE	R Repudiation
CAPEC	CAPEC-169 Footprinting
MDS2	CONN Connectivity capabilities, SBOM Software bill of materials
Standards	IEC 80001-1

CRI-NW-7 Bluetooth from the corridor

† DIRECT HARM THE HOSPITAL · RANK 7

THREAT

Bedside and wearable devices accept Bluetooth connections with weak or no pairing. Someone in the corridor or next bed can crash them, read readings or send commands, and flaws in common Bluetooth chips affect many devices at once.

MITIGATION PROMPTS (ON THE CARD)

1. Which bedside devices accept Bluetooth connections, and how?
2. Could someone in the corridor connect to them?
3. Which common Bluetooth chips do your devices share?

SEEN IN PUBLIC

SweynTooth Bluetooth flaws, 2020. The FDA warned that SweynTooth flaws in Bluetooth Low Energy chips used in pacemakers, glucose monitors, insulin pumps and other devices could let someone nearby crash a device, stop it working or bypass security. Sources: RAPS: FDA warns of cybersecurity vulnerabilities in pacemakers and other BLE devices; HPN: FDA informs about potential vulnerabilities in medical devices with Bluetooth Low Energy

MITIGATION PRINCIPLE

Bluetooth links to clinical devices are authenticated, encrypted and limited to the intended peer.

DESIGN MEASURES

1. Require authenticated pairing with numeric comparison or out-of-band exchange, never just-works for therapy devices.
2. Accept connections only from bonded peers and disable advertising once paired where possible.
3. Track chipset vulnerabilities through the SBOM and patch or shield affected models.

MAPPINGS

STRIDE	S Spoofing, T Tampering, D Denial of service
LINDDUN	DD Data disclosure
CAPEC	CAPEC-667 Bluetooth Impersonation AttackS (BIAS) CAPEC-668 Key Negotiation of Bluetooth Attack (KNOB) CAPEC-666 BlueSmacking
CWE	CWE-940 Improper Verification of Source of a Communication Channel CWE-322 Key Exchange without Entity Authentication
ATT&CK	T1011.001 Exfiltration Over Bluetooth
EMB3D	TID-406 Unauthorized Messages or Connections TID-408 Unencrypted Sensitive Data Communication
MDS2	NAUT Node authentication, TXCF Transmission confidentiality
Standards	FDA premarket IEC TR 60601-4-5

CRI-NW-6 Clocks and names shared with devices

THE HOSPITAL · RANK 6

THREAT

Monitors, pumps and the record depend on hospital DNS, DHCP and time servers built for office IT. A failure or spoof misdirects device data or skews timestamps, so trends, alarms and drug timings are recorded out of order.

MITIGATION PROMPTS (ON THE CARD)

1. Which DNS, DHCP and time servers do devices depend on?
2. Are those services redundant and protected from spoofing?
3. How would skewed timestamps show up in the record?

MITIGATION PRINCIPLE

Clinical devices rely on core network services that are hardened, redundant and authenticated.

DESIGN MEASURES

1. Provide dedicated, redundant DNS, DHCP and time sources for clinical segments.
2. Use authenticated time and pinned server addresses for devices that support them.
3. Alert on clock drift between devices and the record beyond a clinical tolerance.

MAPPINGS

STRIDE	S Spoofing, T Tampering, D Denial of service
CAPEC	CAPEC-142 DNS Cache Poisoning CAPEC-697 DHCP Spoofing
CWE	CWE-350 Reliance on Reverse DNS Resolution for a Security-Critical Action CWE-346 Origin Validation Error
ATT&CK	T1557.003 DHCP Spoofing
MDS2	IGAU Health data integrity and authenticity, CONN Connectivity capabilities
Standards	IEC 80001-1

CRI-NW-5 Live ports in public areas

THE HOSPITAL · RANK 5

THREAT

Network ports in patient rooms, waiting areas and corridors are live and give full access to clinical networks. A visitor or patient plugs in a laptop or small device and reaches monitors and records.

MITIGATION PROMPTS (ON THE CARD)

1. Which network ports in public areas are live?
2. What happens when an unknown device plugs in?
3. Could a visitor's laptop reach a monitor or the record?

MITIGATION PRINCIPLE

Only known, authorised devices can use a network port, and public areas have none that reach clinical networks.

DESIGN MEASURES

1. Enforce network access control on every port, placing unknown devices in an isolated segment.
2. Disable unused ports and patch only what each room needs.
3. Alert on new devices appearing on clinical segments.

MAPPINGS

STRIDE	S Spoofing, E Elevation of privilege
CAPEC	CAPEC-390 Bypassing Physical Security
CWE	CWE-1263 Improper Physical Access Control
ATT&CK	T1200 Hardware Additions
MDS2	CONN Connectivity capabilities, PLOK Physical locks
Standards	IEC 80001-1

CRI-NW-4 Location tags leak movements

THE HOSPITAL · RANK 4

THREAT

Real-time location tags on patients, staff and equipment broadcast identifiers and feed location history to dashboards open to many users. Movements of vulnerable or high-profile patients can be tracked, and spoofed tags send staff looking in the wrong place.

MITIGATION PROMPTS (ON THE CARD)

1. Who can see location history from RTLS dashboards?
2. What purpose justifies tracking each patient or staff tag?
3. How would spoofed tags be detected?

MITIGATION PRINCIPLE

Location data is collected for a stated purpose, protected like clinical data and limited to those who need it.

DESIGN MEASURES

1. Rotate tag identifiers and encrypt tag transmissions where the technology allows.
2. Restrict location views by role and keep history only as long as its purpose needs.
3. Tell patients and staff what is tracked and why.

MAPPINGS

STRIDE	S Spoofing, I Information disclosure
LINDDUN	L Linking, I Identifying, D Detecting, U Unawareness and unintervenability
CAPEC	CAPEC-619 Signal Strength Tracking CAPEC-612 WiFi MAC Address Tracking
CWE	CWE-359 Exposure of Private Personal Information to an Unauthorized Actor
MDS2	MPII Management of private data, TXCF Transmission confidentiality
Standards	ISO 27799

CRI-NW-3 Patient and guest Wi-Fi not isolated

THE HOSPITAL · RANK 3

THREAT

Guest and patient Wi-Fi share infrastructure and routing with clinical networks. A patient's infected laptop, or a device bridging two networks, becomes a path into clinical systems.

MITIGATION PROMPTS (ON THE CARD)

1. How is guest Wi-Fi separated from clinical networks?
2. Could a device bridge guest and clinical networks?
3. What shared infrastructure do both networks use?

MITIGATION PRINCIPLE

Guest networks are isolated from clinical networks in design, not only by configuration.

DESIGN MEASURES

1. Route guest traffic straight to the internet on separate infrastructure or tunnelled VLANs with no internal routes.
2. Enable client isolation on guest Wi-Fi.
3. Test isolation after every network change.

MAPPINGS

STRIDE	E Elevation of privilege
CAPEC	CAPEC-700 Network Boundary Bridging
CWE	CWE-653 Improper Isolation or Compartmentalization
ATT&CK	T1599 Network Boundary Bridging
MDS2	CONN Connectivity capabilities
Standards	IEC 80001-1

CRI-NW-2 Satellite sites trusted completely

THE HOSPITAL · RANK 2

THREAT

Clinics, community sites and partner buildings connect over links with weaker controls, yet the main network trusts them fully. A compromise at the smallest site reaches the main hospital's devices.

MITIGATION PROMPTS (ON THE CARD)

1. What can a small clinic site reach in the main hospital?
2. Which flows from satellite sites are actually required?
3. How are controls at the smallest site checked?

MITIGATION PRINCIPLE

Every site is treated as its own trust zone, with only required flows allowed into the main hospital.

DESIGN MEASURES

1. Terminate site links at enforcement points that filter to documented services.
2. Apply the same device and identity standards at small sites, or limit what they can reach.
3. Monitor inter-site traffic for unexpected protocols.

MAPPINGS

STRIDE	E Elevation of privilege
CAPEC	CAPEC-700 Network Boundary Bridging
CWE	CWE-653 Improper Isolation or Compartmentalization
ATT&CK	T1199 Trusted Relationship
MDS2	CONN Connectivity capabilities
Standards	IEC 80001-1

CRI-CC · THE HOSPITAL · 13 ENTRIES

Clinical Communications

Nurse call, alarm routing to handsets, pagers and bleeps, DECT and Wi-Fi phones, secure and shadow messaging, crash calls, switchboard and overhead paging.

https://ostering.com/taxonomies/hospitals-and-medical-devices/clinical-communications/

CRI-CC-A Alarms that never reach the nurse

† CARE DELAYED OR WRONG THE HOSPITAL · RANK A

THREAT

Monitor and pump alarms travel through middleware to nurses' handsets, with no end-to-end confirmation of delivery. When the middleware fails, is misconfigured or is tampered with, alarms vanish while every system shows normal.

MITIGATION PROMPTS (ON THE CARD)

1. How is delivery of an alarm to a handset confirmed?
2. What happens when an alarm is not acknowledged in time?
3. Would anyone notice the middleware had stopped forwarding alarms?

MITIGATION PRINCIPLE

Every clinical alarm is confirmed as delivered and acknowledged, and escalates when it is not.

DESIGN MEASURES

1. Require acknowledgement within a set time and escalate unacknowledged alarms to another clinician and the central station.
2. Monitor the middleware with end-to-end test alarms and alert on any failure to deliver.
3. Keep audible bedside and central alarms active as a backstop whatever the middleware does.

MAPPINGS

STRIDE	T Tampering, D Denial of service, R Repudiation
CAPEC	CAPEC-603 Blockage
CWE	CWE-392 Missing Report of Error Condition CWE-754 Improper Check for Unusual or Exceptional Conditions
ATT&CK	T0878 Alarm Suppression T0815 Denial of View
MDS2	IGAU Health data integrity and authenticity, AUDT Audit controls
Standards	IEC 80001-1 ISO 14971

CRI-CC-K Crash calls on one platform

† CARE DELAYED OR WRONG THE HOSPITAL · RANK K

THREAT

The cardiac arrest and rapid response call path runs on the same IP telephony and network as everything else. When ransomware or an outage takes it down, staff cannot summon the resuscitation team.

MITIGATION PROMPTS (ON THE CARD)

1. What carries a crash call from the handset to every team bleep?
2. How does the caller know the team was reached?
3. What is the fallback, and when was it last tested?

MITIGATION PRINCIPLE

Emergency call paths have an independent fallback that works when the main network and telephony are down.

DESIGN MEASURES

1. Provide an independent backup for crash and emergency calls, such as dedicated lines, radios or hard-wired alarms.
2. Test the emergency call path daily, end to end, and log the result.
3. Train staff on the downtime method and display it at every call point.

MAPPINGS

STRIDE	D Denial of service
CAPEC	CAPEC-603 Blockage
CWE	CWE-1357 Reliance on Insufficiently Trustworthy Component
ATT&CK	T1489 Service Stop T1498 Network Denial of Service
MDS2	DTBK Data backup and disaster recovery, CONN Connectivity capabilities
Standards	IEC 80001-1

CRI-CC-Q Nurse call failing silently

† CARE DELAYED OR WRONG THE HOSPITAL · RANK Q

THREAT

IP nurse call systems sit on shared networks with default settings. A fault or attack stops patient calls from reaching staff, or marks them answered, and patients who cannot leave their bed have no other way to get help.

MITIGATION PROMPTS (ON THE CARD)

1. How would staff know nurse call had stopped working?
2. What does a patient who can't leave the bed do if it fails?
3. Who monitors nurse call as a safety system?

MITIGATION PRINCIPLE

Nurse call is designed and monitored as a patient-safety system with a known fallback.

DESIGN MEASURES

1. Supervise every call point and alert on lost connections or stuck states.
2. Isolate nurse call on its own segment and harden its servers and default accounts.
3. Define ward procedures, such as increased rounding, for when nurse call is degraded.

MAPPINGS

STRIDE	T Tampering, D Denial of service
CAPEC	CAPEC-176 Configuration/Environment Manipulation
CWE	CWE-1392 Use of Default Credentials CWE-754 Improper Check for Unusual or Exceptional Conditions
ATT&CK	T0814 Denial of Service
MDS2	SAHD System and application hardening, CONN Connectivity capabilities
Standards	IEC 80001-1

CRI-CC-J False alarms and fake calls

† CARE DELAYED OR WRONG THE HOSPITAL · RANK J

THREAT

Handsets and paging accept alarms and messages from anything that can reach the messaging gateway. Injected false alarms or fake emergency calls send staff to the wrong bed, mask real alarms and wear down trust in the system.

MITIGATION PROMPTS (ON THE CARD)

1. Which systems can send alarms or calls to handsets?
2. Can staff see where an alarm or emergency call came from?
3. How would injected false alarms be spotted and stopped?

MITIGATION PRINCIPLE

Only authenticated systems can raise alarms and emergency calls, and staff can see where each came from.

DESIGN MEASURES

1. Authenticate every system that can send to the alarm and messaging gateway, and reject the rest.
2. Show the source device, location and patient on every alarm so staff can judge it quickly.
3. Alert on unusual alarm volumes or sources.

MAPPINGS

STRIDE	S Spoofing, T Tampering
CAPEC	CAPEC-148 Content Spoofing CAPEC-151 Identity Spoofing
CWE	CWE-306 Missing Authentication for Critical Functionality CWE-940 Improper Verification of Source of a Communication Channel
ATT&CK	T1565.002 Transmitted Data Manipulation
MDS2	NAUT Node authentication, TXIG Transmission integrity
Standards	IEC 80001-1

CRI-CC-10 Pages read and spoofed by radio

THE HOSPITAL · RANK 10

THREAT

Pagers and bleeps carry patient names, conditions and locations unencrypted over radio. Anyone with a cheap receiver can read them, and anyone with a transmitter can send pages that look genuine.

MITIGATION PROMPTS (ON THE CARD)

1. What patient details appear in pager messages?
2. Could a cheap receiver read your hospital's pages?
3. How would a spoofed page be told from a genuine one?

SEEN IN PUBLIC

Leaking Beeps, 2016. Trend Micro research showed that pager messages sent by US hospitals were unencrypted and could be read with cheap radio equipment, exposing patient names, diagnoses and treatment details. Sources: Trend Micro: Leaking Beeps, unencrypted pager messages in the healthcare industry; Trend Micro: Are pagers leaking your patients' PHI?

MITIGATION PRINCIPLE

Paging carries no patient-identifiable data in the clear, and pages that start clinical action are authenticated.

DESIGN MEASURES

1. Move clinical paging to encrypted, authenticated messaging, or strip patient details from pages.
2. Use pages only as a call-back prompt, with clinical detail given on a verified channel.
3. Plan retirement of unencrypted paging, keeping a resilient alert method in its place.

MAPPINGS

STRIDE	S Spoofing, I Information disclosure
LINDDUN	DD Data disclosure, I Identifying
CAPEC	CAPEC-157 Sniffing Attacks CAPEC-148 Content Spoofing
CWE	CWE-319 Cleartext Transmission of Sensitive Information CWE-290 Authentication Bypass by Spoofing
ATT&CK	T1040 Network Sniffing
MDS2	TXCF Transmission confidentiality, TXIG Transmission integrity
Standards	ISO 27799

CRI-CC-9 Clinical care on consumer messaging

THE HOSPITAL · RANK 9

THREAT

When official tools are slow, clinicians share patient photos, results and decisions in consumer messaging groups on personal phones. Data sits outside the record and the hospital, with no audit, retention or way to remove it.

MITIGATION PROMPTS (ON THE CARD)

1. Why do clinicians reach for consumer messaging instead?
2. How do decisions made in messages reach the record?
3. What happens to patient photos on personal phones?

MITIGATION PRINCIPLE

Official clinical messaging is quicker than the shadow alternative, and decisions made in it reach the record.

DESIGN MEASURES

1. Provide an approved secure messaging app that handles photos and groups as easily as consumer apps.
2. Write messaging decisions back to the record automatically or prompt for it.
3. Set clear guidance, and remove clinical content from personal devices when staff leave.

MAPPINGS

STRIDE	I Information disclosure, R Repudiation
LINDDUN	DD Data disclosure, U Unawareness and unintervenability, Nc Non-compliance
CAPEC	CAPEC-545 Pull Data from System Resources
CWE	CWE-359 Exposure of Private Personal Information to an Unauthorized Actor CWE-213 Exposure of Sensitive Information Due to Incompatible Policies
ATT&CK	T1213.005 Messaging Applications
MDS2	MPII Management of private data, STCF Data storage confidentiality
Standards	ISO 27799

CRI-CC-8 Impersonating a clinician by message

† CARE DELAYED OR WRONG THE HOSPITAL · RANK 8

THREAT

Secure messaging trusts the display name. Anyone with a hijacked account, or a lookalike profile, can send orders, ask for results or request a change in treatment, and the recipient acts on it.

MITIGATION PROMPTS (ON THE CARD)

1. How does a recipient verify who sent a clinical message?
2. Which requests need confirming on a second channel?
3. What could a hijacked messaging account ask for?

MITIGATION PRINCIPLE

Clinical instructions sent by message come from verified identities, and high-risk requests are confirmed on a second channel.

DESIGN MEASURES

1. Tie messaging accounts to verified staff identity, with phishing-resistant authentication.
2. Show role and verification status clearly, and flag external or newly created accounts.
3. Require a call-back or order entry for high-risk instructions such as drug or dose changes.

MAPPINGS

STRIDE	S Spoofing, R Repudiation
CAPEC	CAPEC-151 Identity Spoofing CAPEC-98 Phishing
CWE	CWE-290 Authentication Bypass by Spoofing CWE-308 Use of Single-factor Authentication
ATT&CK	T1566.003 Spearphishing via Service T1534 Internal Spearphishing
MDS2	PAUT Person authentication, AUTH Authorization
Standards	IEC 80001-1

CRI-CC-7 Switchboard and rota as weak link

† CARE DELAYED OR WRONG THE HOSPITAL · RANK 7

THREAT

Switchboard, on-call rotas and contact directories decide who gets called. A tampered rota or a convincing caller sends emergency calls to the wrong person, or obtains direct numbers and patient whereabouts.

MITIGATION PROMPTS (ON THE CARD)

1. Who can edit on-call rotas and the staff directory?
2. What verification does switchboard apply to unusual callers?
3. How would a tampered rota be noticed during the night?

MITIGATION PRINCIPLE

Rotas and directories are controlled data, and switchboard follows verification scripts.

DESIGN MEASURES

1. Restrict and log edits to on-call rotas and contact directories, with change alerts to the owning team.
2. Give switchboard staff verification scripts for requests about patients or staff.
3. Check critical rotas automatically against expected coverage before each shift.

MAPPINGS

STRIDE	S Spoofing, T Tampering
LINDDUN	DD Data disclosure
CAPEC	CAPEC-415 Pretexting via Phone CAPEC-407 Pretexting
CWE	CWE-732 Incorrect Permission Assignment for Critical Resource
ATT&CK	T1566.004 Spearphishing Voice
MDS2	AUTH Authorization, AUDT Audit controls

CRI-CC-6 Shared handsets with no owner

† CARE DELAYED OR WRONG THE HOSPITAL · RANK 6

THREAT

Ward handsets are passed between staff without login. Whoever holds one sees patient alarms and messages and can acknowledge them, and there is no record of who did.

MITIGATION PROMPTS (ON THE CARD)

1. How do you know who held a handset when an alarm was acknowledged?
2. Do staff sign in to ward handsets at handover?
3. What can someone holding a spare handset see and do?

MITIGATION PRINCIPLE

Each alarm acknowledgement is tied to the person holding the handset at the time.

DESIGN MEASURES

1. Require quick sign-in to handsets at shift start, by badge or code, and sign out on dock.
2. Record who acknowledged every alarm and message.
3. Hide message content on the lock screen and wipe handsets on return.

MAPPINGS

STRIDE	S Spoofing, R Repudiation, I Information disclosure
LINDDUN	DD Data disclosure, Nr Non-repudiation
CAPEC	CAPEC-122 Privilege Abuse
CWE	CWE-308 Use of Single-factor Authentication CWE-1463 Insufficient Session Timeout Value
MDS2	PAUT Person authentication, ALOF Automatic logoff, AUDT Audit controls

CRI-CC-5 Overhead paging hijacked

THE HOSPITAL · RANK 5

THREAT

Overhead paging and public address systems are now IP-based and reachable from the wider network. A false emergency code or evacuation announcement can cause panic or disrupt care across a site.

MITIGATION PROMPTS (ON THE CARD)

1. Which consoles and systems can trigger overhead announcements?
2. How is an emergency announcement authenticated?
3. What would a false evacuation code cost the site?

MITIGATION PRINCIPLE

Public address is reachable only from authorised consoles, and emergency announcements need authenticated sources.

DESIGN MEASURES

1. Isolate the PA system and permit only named consoles to broadcast.
2. Require authentication for emergency and evacuation announcements.
3. Log every broadcast and alert on unexpected sources.

MAPPINGS

STRIDE	S Spoofing, D Denial of service
CAPEC	CAPEC-148 Content Spoofing
CWE	CWE-306 Missing Authentication for Critical Functionality
MDS2	AUTH Authorization, CONN Connectivity capabilities

CRI-CC-4 Clinical apps on personal phones

THE HOSPITAL · RANK 4

THREAT

Staff run clinical messaging and record apps on their own phones without device management. Lost or shared phones expose patient data on lock screens, in backups and in notifications.

MITIGATION PROMPTS (ON THE CARD)

1. What patient data shows on lock screens and notifications?
2. Do clinical apps protect their data on unmanaged phones?
3. What happens to app data when a phone is lost?

MITIGATION PRINCIPLE

Clinical apps protect their own data, whatever device they run on.

DESIGN MEASURES

1. Use app-level protection: separate PIN, encrypted storage and remote wipe of app data.
2. Hide clinical content from notifications and exclude it from personal backups.
3. Require a minimum operating system version and screen lock to run clinical apps.

MAPPINGS

STRIDE	I Information disclosure
LINDDUN	DD Data disclosure
CAPEC	CAPEC-507 Physical Theft
CWE	CWE-312 Cleartext Storage of Sensitive Information CWE-359 Exposure of Private Personal Information to an Unauthorized Actor
ATT&CK	T1005 Data from Local System
MDS2	STCF Data storage confidentiality, ALOF Automatic logoff
Standards	ISO 27799

CRI-CC-3 Status boards in public view

THE HOSPITAL · RANK 3

THREAT

Electronic whiteboards and patient status screens show names, diagnoses and risks where visitors can see them, and some can be edited from any ward PC without login.

MITIGATION PROMPTS (ON THE CARD)

1. What do status boards show that visitors can read?
2. Who can edit a status board, and is a login required?
3. Which details could be removed without hurting care?

MITIGATION PRINCIPLE

Status displays show only what the audience needs, and edits are authenticated.

DESIGN MEASURES

1. Use initials or bed numbers on displays visible to the public.
2. Require authenticated edits and log changes to patient status.
3. Position screens and set privacy modes by location.

MAPPINGS

STRIDE	I Information disclosure, T Tampering
LINDDUN	DD Data disclosure, I Identifying
CAPEC	CAPEC-699 Eavesdropping on a Monitor
CWE	CWE-359 Exposure of Private Personal Information to an Unauthorized Actor CWE-862 Missing Authorization
MDS2	MPII Management of private data, AUTH Authorization

CRI-CC-2 Recordings with clinical detail

THREAT

Call recordings, voicemail and message archives hold clinical conversations, kept indefinitely and readable by telephony administrators and suppliers.

MITIGATION PROMPTS (ON THE CARD)

1. How long are call recordings and voicemail kept?
2. Who can listen to archived clinical conversations?
3. Do suppliers have access to communication archives?

MITIGATION PRINCIPLE

Communications records are kept for a defined purpose and period, under clinical data protection.

DESIGN MEASURES

1. Set retention limits for recordings and archives and purge on schedule.
2. Encrypt recordings and limit access by role, with audit.
3. Include telephony suppliers in data protection agreements.

MAPPINGS

STRIDE	I Information disclosure
LINDDUN	DD Data disclosure, Nc Non-compliance
CAPEC	CAPEC-545 Pull Data from System Resources
CWE	CWE-312 Cleartext Storage of Sensitive Information
ATT&CK	T1123 Audio Capture
MDS2	STCF Data storage confidentiality, MPII Management of private data
Standards	ISO 27799

CRI-EC · THE HOSPITAL · 13 ENTRIES

Emergency and External Communications

Ambulance dispatch, prehospital ECG and pre-alerts, emergency services radio, diversion, image transfer, telehealth, hospital-at-home hubs, staff call-in, patient SMS and backup links.

https://ostering.com/taxonomies/hospitals-and-medical-devices/emergency-and-external-communications/

CRI-EC-A Dispatch links fail without warning

† CARE DELAYED OR WRONG THE HOSPITAL · RANK A

THREAT

Ambulance dispatch, hospital status and handover links run over one integration path that nobody monitors end to end. When it fails or is taken down, crews and emergency departments keep working from stale information, ambulances queue or go to the wrong place, and no one notices until patients are harmed.

MITIGATION PROMPTS (ON THE CARD)

1. Who monitors the dispatch link to the hospital end to end?
2. How would both control rooms know the link had gone quiet?
3. What fallback for status and pre-alerts shares none of its failure?

SEEN IN PUBLIC

Advanced and NHS 111, 2022. Ransomware at software supplier Advanced disrupted the Adastra system used by NHS 111 and out-of-hours services, and exposed data on about 80,000 people. The UK Information Commissioner fined Advanced £3.07 million in March 2025. Sources: ICO: Software provider fined £3m following 2022 ransomware attack

MITIGATION PRINCIPLE

Every link between dispatch and the hospital is monitored end to end and has a rehearsed fallback that does not share its failure.

DESIGN MEASURES

1. Send heartbeat messages across each dispatch and handover link and alarm in both control rooms when one goes quiet.
2. Keep a voice and radio fallback for status and pre-alerts on separate infrastructure, with numbers held offline.
3. Rehearse loss of the dispatch link jointly with the ambulance service at least yearly, including the switch back.

MAPPINGS

STRIDE	D Denial of service
CAPEC	CAPEC-582 Route Disabling CAPEC-607 Obstruction
CWE	CWE-754 Improper Check for Unusual or Exceptional Conditions CWE-1320 Improper Protection for Outbound Error Messages and Alert Signals
ATT&CK	T1489 Service Stop T1498 Network Denial of Service
MDS2	DTBK Data backup and disaster recovery, CONN Connectivity capabilities
Standards	IEC 80001-1

CRI-EC-K Diversion status falsified or stale

† CARE DELAYED OR WRONG THE HOSPITAL · RANK K

THREAT

Regional capacity and diversion boards accept status changes from any logged-in user or unauthenticated feed. A false closed sends ambulances past the nearest capable hospital; a false open sends a stroke or trauma patient to a hospital whose scanner or theatre is down.

MITIGATION PROMPTS (ON THE CARD)

1. Who can change a hospital's diversion status, and how is it confirmed?
2. Does the board show how old each status is?
3. What happens when a status feed is unauthenticated or stale?

SEEN IN PUBLIC

University Hospital Düsseldorf, 2020. Ransomware took down systems at University Hospital Düsseldorf and it stopped taking emergency admissions; a woman sent to a hospital in another city died. Prosecutors opened a homicide inquiry but closed it, concluding her condition alone caused her death and the delay did not affect the outcome. Sources: MIT Technology Review: A patient has died after ransomware hackers hit a German hospital; Born's Tech and Windows World: ransomware at Uniklinik Düsseldorf not responsible for death

Ascension, 2024. A ransomware attack took Ascension's electronic health records offline across its hospitals, staff worked on paper and some ambulances were diverted; data on about 5.6 million people was taken. Sources: BleepingComputer: Ascension health data of 5.6 million stolen in ransomware attack

MITIGATION PRINCIPLE

Diversion status is changed only by named, authorised people, is confirmed out of band, and shows its age.

DESIGN MEASURES

1. Require named authentication and a second confirmation by phone before a hospital's diversion status changes.
2. Show the time and author of every status change on the board, and mark status older than a set period as stale.
3. Publish service-level status (CT, cath lab, theatres) separately from whole-site diversion so crews route by capability.

MAPPINGS

STRIDE	S Spoofing, T Tampering, R Repudiation
CAPEC	CAPEC-148 Content Spoofing CAPEC-194 Fake the Source of Data
CWE	CWE-306 Missing Authentication for Critical Functionality CWE-863 Incorrect Authorization
ATT&CK	T1565.001 Stored Data Manipulation T1078 Valid Accounts
MDS2	AUTH Authorization, AUDT Audit controls, IGAU Health data integrity and authenticity

CRI-EC-Q Prehospital ECG and pre-alert tampered

† CARE DELAYED OR WRONG THE HOSPITAL · RANK Q

THREAT

Twelve-lead ECGs and stroke or trauma pre-alerts travel from the ambulance to the hospital by fax, email, messaging or a vendor cloud without integrity or patient binding. An altered, delayed or misattributed tracing means the cath lab or stroke team is not activated, or is activated for the wrong patient.

MITIGATION PROMPTS (ON THE CARD)

1. How is a prehospital ECG bound to the right patient and incident?
2. Who confirms that a pre-alert has actually arrived?
3. Which routes carry tracings: fax, email, messaging or vendor cloud?

MITIGATION PRINCIPLE

Prehospital clinical data is signed at source, bound to the patient and incident, and its delivery is confirmed by a person.

DESIGN MEASURES

1. Sign ECGs on the monitor or gateway and verify the signature before display in the hospital.
2. Bind each transmission to an incident number and patient identifiers, and show both prominently to the receiving clinician.
3. Require a spoken acknowledgement of time-critical pre-alerts and alarm the crew when none arrives in time.

MAPPINGS

STRIDE	S Spoofing, T Tampering, I Information disclosure
LINDDUN	L Linking, DD Data disclosure
CAPEC	CAPEC-94 Adversary in the Middle (AiTM) CAPEC-148 Content Spoofing
CWE	CWE-924 Improper Enforcement of Message Integrity During Transmission in a Communication Channel CWE-319 Cleartext Transmission of Sensitive Information CWE-353 Missing Support for Integrity Check
ATT&CK	T1565.002 Transmitted Data Manipulation T1557 Adversary-in-the-Middle
EMB3D	TID-408 Unencrypted Sensitive Data Communication
MDS2	TXIG Transmission integrity, TXCF Transmission confidentiality, NAUT Node authentication
Standards	IEC 81001-5-1

CRI-EC-J Emergency services radio jammed or spoofed

† CARE DELAYED OR WRONG THE HOSPITAL · RANK J

THREAT

Ambulance crews rely on one radio system for clinical advice, backup and handover, with no tested alternative. Jamming, a rogue transmitter or loss of the radio core leaves crews unable to call for help or receive changed instructions, and spoofed traffic can send them to false incidents.

MITIGATION PROMPTS (ON THE CARD)

1. What second way do crews have to reach control?
2. How is a radio instruction that changes destination verified?
3. What would crews do if the radio core went down?

MITIGATION PRINCIPLE

Crews keep at least two independent ways to reach control, and voice instructions that change a destination are verified.

DESIGN MEASURES

1. Provide a second bearer, such as cellular with priority access or satellite, that does not share the radio core or sites.
2. Detect and report interference by monitoring receiver noise at base sites and from vehicles.
3. Verify destination changes received by voice through the vehicle's data terminal or a call-back procedure.

MAPPINGS

STRIDE	S Spoofing, D Denial of service
CAPEC	CAPEC-601 Jamming CAPEC-599 Terrestrial Jamming CAPEC-605 Cellular Jamming
CWE	CWE-940 Improper Verification of Source of a Communication Channel
MDS2	CONN Connectivity capabilities

CRI-EC-10 Emergency call handoff flooded or faked

† CARE DELAYED OR WRONG THE HOSPITAL · RANK 10

THREAT

The interface that passes calls and incident data from the emergency call centre to ambulance dispatch trusts every record it receives and has no limit on volume. A flood of fake calls or injected incidents exhausts call-takers and ambulances, and real emergencies wait.

MITIGATION PROMPTS (ON THE CARD)

1. How does dispatch know an incident record came from the call centre?
2. What limits the volume of incidents the handoff accepts?
3. Could operators spot a coordinated flood of fake calls?

MITIGATION PRINCIPLE

Incident handoff between call centres and dispatch authenticates its source, limits volume and lets operators spot coordinated floods.

DESIGN MEASURES

1. Authenticate each system that can create incidents in dispatch and reject records from anything else.
2. Rate-limit and alarm on surges of calls or incidents from one number range, route or interface.
3. Keep a surge procedure that lets clinicians triage queued calls by risk when volume is abnormal.

MAPPINGS

STRIDE	S Spoofing, D Denial of service
CAPEC	CAPEC-125 Flooding CAPEC-194 Fake the Source of Data
CWE	CWE-770 Allocation of Resources Without Limits or Throttling CWE-940 Improper Verification of Source of a Communication Channel
ATT&CK	T1498 Network Denial of Service T1499.003 Application Exhaustion Flood
MDS2	NAUT Node authentication, AUDT Audit controls

CRI-EC-9 Image transfer between hospitals unverified

† CARE DELAYED OR WRONG THE HOSPITAL · RANK 9

THREAT

Image-sharing links between hospitals accept studies from any connected peer and import them straight into the local archive. A wrong-patient study, an altered image or a DICOM file carrying malware arrives with the trust of a referral, and when the link is down a time-critical neurosurgical or trauma referral stalls.

MITIGATION PROMPTS (ON THE CARD)

1. Which hospitals can push images straight into your archive?
2. Who matches an incoming study to the right patient?
3. What happens to a time-critical referral when the link is down?

SEEN IN PUBLIC

DICOM files carrying malware, 2019. Cylera researchers showed that the DICOM file format allows an image file to also be a working Windows executable, so malware could hide inside medical images protected as patient data (CVE-2019-11687). Sources: NVD: CVE-2019-11687; GovInfoSecurity: Researchers, malware can be hidden in medical images

MITIGATION PRINCIPLE

Images from other organisations are authenticated, matched to the patient by a person, and checked before they enter the local archive.

DESIGN MEASURES

1. Authenticate each sending organisation and node, and keep a list of peers allowed to send.
2. Quarantine imported studies until patient identity is reconciled and files are scanned for embedded executable content.
3. Keep a tested secondary route for urgent referrals, such as a separate image-sharing service, with known contacts.

MAPPINGS

STRIDE	S Spoofing, T Tampering, D Denial of service
LINDDUN	L Linking, DD Data disclosure
CAPEC	CAPEC-148 Content Spoofing CAPEC-636 Hiding Malicious Data or Code within Files
CWE	CWE-353 Missing Support for Integrity Check CWE-349 Acceptance of Extraneous Untrusted Data With Trusted Data
ATT&CK	T1565.002 Transmitted Data Manipulation T1204.002 Malicious File
MDS2	NAUT Node authentication, IGAU Health data integrity and authenticity, MLDP Malware detection and protection
Standards	DICOM PS3.15

CRI-EC-8 Hospital-at-home hub goes blind

† CARE DELAYED OR WRONG THE HOSPITAL · RANK 8

THREAT

Virtual wards depend on one monitoring hub that gathers observations from patients' homes through a vendor platform and mobile networks. If the hub, platform or feed fails or is tampered with, deteriorating patients look stable and nobody is called, because silence reads as normal.

MITIGATION PROMPTS (ON THE CARD)

1. Does the virtual ward treat missing observations as an alarm?
2. How would staff reach every patient if the platform failed?
3. Which links between home and hub could fail silently?

MITIGATION PRINCIPLE

A virtual ward treats missing data as an alarm and keeps a way to reach every patient when the platform fails.

DESIGN MEASURES

1. Alarm on each patient whose readings stop arriving within the expected interval, not only on abnormal readings.
2. Keep an offline list of virtual-ward patients with phone numbers and escalation plans, refreshed every shift.
3. Restrict who can change alert thresholds and log every change with the reason and clinician.

MAPPINGS

STRIDE	T Tampering, D Denial of service, R Repudiation
LINDDUN	DD Data disclosure
CAPEC	CAPEC-607 Obstruction CAPEC-148 Content Spoofing
CWE	CWE-754 Improper Check for Unusual or Exceptional Conditions CWE-1320 Improper Protection for Outbound Error Messages and Alert Signals
ATT&CK	T1565.001 Stored Data Manipulation T1489 Service Stop
MDS2	DTBK Data backup and disaster recovery, AUDT Audit controls, AUTH Authorization
Standards	IEC 80001-1

CRI-EC-7 Staff call-in cascade abused

THE HOSPITAL · RANK 7

THREAT

Major-incident and staff call-in messages go out by SMS or automated calls that anyone can imitate, and the cascade platform has weak login. A false major incident pulls staff in and drains the next shift; a blocked or hijacked cascade leaves the hospital short when a real one starts.

MITIGATION PROMPTS (ON THE CARD)

1. How can staff tell a genuine call-in message from a fake?
2. Who can log in to the cascade platform, and how?
3. What is the manual fallback if the cascade is blocked?

MITIGATION PRINCIPLE

Call-in messages are verifiable by staff, the cascade is protected like a clinical system, and a manual fallback exists.

DESIGN MEASURES

1. Tell staff how genuine call-ins look and give them a number or app to confirm one before travelling.
2. Protect the cascade platform with multi-factor login and two-person activation for a major incident.
3. Hold printed call-in trees and a switchboard procedure for when the platform is down.

MAPPINGS

STRIDE	S Spoofing, D Denial of service
CAPEC	CAPEC-148 Content Spoofing CAPEC-416 Manipulate Human Behavior
CWE	CWE-308 Use of Single-factor Authentication CWE-290 Authentication Bypass by Spoofing
ATT&CK	T1684.001 Impersonation T1078 Valid Accounts
MDS2	PAUT Person authentication, AUTH Authorization

CRI-EC-6 Telehealth consult hijacked or impersonated

† CARE DELAYED OR WRONG THE HOSPITAL · RANK 6

THREAT

Video and phone consultations use reusable links and no identity check on either side. Someone can join or take over a consult, impersonate the clinician to give harmful advice or extract details, or impersonate the patient to obtain prescriptions and records.

MITIGATION PROMPTS (ON THE CARD)

1. How are the clinician and the patient each identified on a remote consult?
2. Are session links single-use and tied to the appointment?
3. Could someone join a consult without anyone noticing?

MITIGATION PRINCIPLE

Both parties in a remote consultation are identified, and session links are single-use and bound to the appointment.

DESIGN MEASURES

1. Issue single-use, time-limited links bound to the appointment, and lock the room once both parties join.
2. Verify the patient's identity at the start of each consult and record that it was done.
3. Show the clinician's verified name and organisation in the client, and give patients a way to confirm it.

MAPPINGS

STRIDE	S Spoofing, I Information disclosure, E Elevation of privilege
LINDDUN	I Identifying, DD Data disclosure, D Detecting
CAPEC	CAPEC-593 Session Hijacking CAPEC-151 Identity Spoofing
CWE	CWE-308 Use of Single-factor Authentication CWE-1467 Use of Singular Authentication Artifact for Multiple User Sessions
ATT&CK	T1684.001 Impersonation
MDS2	PAUT Person authentication, TXCF Transmission confidentiality
Standards	ISO 27799

CRI-EC-5 Ambulance location depends on GNSS

† CARE DELAYED OR WRONG THE HOSPITAL · RANK 5

THREAT

Ambulance location, nearest-vehicle allocation and timestamps on care records depend on GNSS. Jamming or spoofing near a station or along a route misplaces vehicles, sends a distant crew to a cardiac arrest, and leaves records with wrong times.

MITIGATION PROMPTS (ON THE CARD)

1. What other source confirms ambulance position besides GNSS?
2. How are implausible vehicle positions flagged before allocation?
3. Which records take their timestamps from GNSS?

MITIGATION PRINCIPLE

Vehicle location and time come from more than one source, and implausible positions are flagged before allocation.

DESIGN MEASURES

1. Combine GNSS with cellular location and vehicle odometry, and flag positions that jump or freeze.
2. Let dispatchers override automated allocation when location quality is flagged as poor.
3. Take care-record timestamps from a trusted network time source, with GNSS only as a fallback.

MAPPINGS

STRIDE	S Spoofing, T Tampering, D Denial of service
CAPEC	CAPEC-627 Counterfeit GPS Signals CAPEC-628 Carry-Off GPS Attack CAPEC-599 Terrestrial Jamming
CWE	CWE-348 Use of Less Trusted Source CWE-346 Origin Validation Error
MDS2	IGAU Health data integrity and authenticity

CRI-EC-4 Patients trained to click hospital links

THE HOSPITAL · RANK 4

THREAT

Hospitals send appointment reminders, results notices and payment requests by SMS and email with links, from senders anyone can imitate. Patients learn to trust them, so fake messages, fake portals and fake public notices harvest credentials, take payments or tell people the emergency department is closed.

MITIGATION PROMPTS (ON THE CARD)

1. How can patients tell a genuine hospital message from a fake?
2. Do any hospital messages ask patients to log in or pay by link?
3. How would you warn the public about fake hospital notices?

MITIGATION PRINCIPLE

Patients can tell genuine hospital messages from fakes, and messages never ask them to log in or pay through a link.

DESIGN MEASURES

1. Register sender IDs and domains, and publish how genuine messages look and what they will never ask for.
2. Point patients to the portal or app by name instead of sending login links in messages.
3. Monitor for look-alike domains, sender IDs and social accounts, and publish service status only on known channels.

MAPPINGS

STRIDE	S Spoofing, I Information disclosure
LINDDUN	DD Data disclosure, U Unawareness and unintervenability
CAPEC	CAPEC-98 Phishing CAPEC-543 Counterfeit Websites CAPEC-630 TypoSquatting
CWE	CWE-451 User Interface (UI) Misrepresentation of Critical Information
ATT&CK	T1566.002 Spearphishing Link T1583.001 Domains

CRI-EC-3 Ambulance care records leak or lag

THE HOSPITAL · RANK 3

THREAT

Electronic patient care records live on crew tablets and sync through a vendor cloud. When the sync fails at handover the emergency department works from a verbal summary, and a lost or poorly managed tablet exposes records of everyone the crew treated.

MITIGATION PROMPTS (ON THE CARD)

1. What happens at handover when the care record fails to sync?
2. How are crew tablets protected if one is lost?
3. How long do records stay on the tablet after handover?

MITIGATION PRINCIPLE

Prehospital records reach the receiving hospital reliably and are protected on the device for as long as they are held.

DESIGN MEASURES

1. Encrypt records on the tablet, enrol tablets in device management, and remote-wipe on loss.
2. Hand over a printable or local copy of the record when the cloud sync has not completed.
3. Purge records from the tablet once the hospital has acknowledged receipt.

MAPPINGS

STRIDE	I Information disclosure, D Denial of service
LINDDUN	DD Data disclosure, I Identifying
CAPEC	CAPEC-507 Physical Theft
CWE	CWE-312 Cleartext Storage of Sensitive Information
ATT&CK	T1005 Data from Local System
MDS2	STCF Data storage confidentiality, TXCF Transmission confidentiality, DTBK Data backup and disaster recovery
Standards	ISO 27799

CRI-EC-2 Backup radio and satellite never tested

THE HOSPITAL · RANK 2

THREAT

Satellite phones, backup radio and spare lines sit in a cupboard with flat batteries, expired subscriptions and outdated numbers. On the day every other channel fails, the hospital cannot reach the ambulance service, neighbouring hospitals or its own staff.

MITIGATION PROMPTS (ON THE CARD)

1. When were backup radio and satellite phones last used in anger or drill?
2. Who keeps fallback directories current and offline?
3. Are subscriptions, batteries and numbers checked on a schedule?

MITIGATION PRINCIPLE

Fallback communications are part of routine operations, tested on a schedule, and their directories are kept current offline.

DESIGN MEASURES

1. Test every fallback channel monthly with a real call to the ambulance service and a neighbouring hospital.
2. Keep batteries charged, subscriptions in force, and a printed directory beside each device.
3. Name who owns each fallback device and include its use in major-incident exercises.

MAPPINGS

STRIDE	D Denial of service
CWE	CWE-1329 Reliance on Component That is Not Updateable

CRI-FB · THE HOSPITAL · 13 ENTRIES

Facilities and Building Systems

Medical gases, theatre and isolation ventilation, backup power, cold storage, water, sterile services, pneumatic tubes, lifts, infant security and building management.

https://ostering.com/taxonomies/hospitals-and-medical-devices/facilities-and-building-systems/

CRI-FB-A Medical gas alarms suppressed or altered

† DIRECT HARM THE HOSPITAL · RANK A

THREAT

Oxygen and other medical gas plant, pressure monitoring and area alarm panels are networked for remote monitoring with weak or no authentication. Changing pressures or suppressing alarms can starve a ward of oxygen or vacuum without anyone at the panel or on the ward being told.

MITIGATION PROMPTS (ON THE CARD)

1. Which medical gas alarms and pressures can be changed over the network?
2. What local protection works whatever the network says?
3. Would ward staff learn of a gas fault if the panel were silenced?

MITIGATION PRINCIPLE

Medical gas safety depends on local engineered protections and alarms that no network command can disable.

DESIGN MEASURES

1. Keep pressure relief, low-pressure alarms and manifold changeover hardwired, independent of the monitoring network.
2. Make remote monitoring read-only, and route any remote control through an authenticated, logged path that operators approve.
3. Alarm on loss of the monitoring link itself, and test area alarms against the plant on a schedule.

MAPPINGS

STRIDE	T Tampering, D Denial of service
CAPEC	CAPEC-212 Functionality Misuse
CWE	CWE-306 Missing Authentication for Critical Functionality CWE-636 Not Failing Securely
ATT&CK	T0838 Modify Alarm Settings T0878 Alarm Suppression T0836 Modify Parameter
EMB3D	TID-310 Remotely Accessible Unauthenticated Services
MDS2	AUTH Authorization, AUDT Audit controls
Standards	IEC 62443

CRI-FB-K Theatre and isolation pressure reversed

† DIRECT HARM THE HOSPITAL · RANK K

THREAT

Building management controls the air changes and pressure regimes of theatres and isolation rooms. A changed setpoint or schedule turns a negative-pressure room positive or cuts theatre air changes, spreading airborne infection or raising surgical site infection, with displays still showing normal.

MITIGATION PROMPTS (ON THE CARD)

1. What measures room pressure independently of building management?
2. Who can change setpoints or schedules for theatres and isolation rooms?
3. Where would staff see that a negative-pressure room had reversed?

MITIGATION PRINCIPLE

Critical-room pressure and air changes are monitored independently of the system that controls them, at the room.

DESIGN MEASURES

1. Fit independent pressure monitors with local alarms at each isolation room and theatre.
2. Lock critical-room setpoints and schedules, requiring authenticated, logged changes with an engineering approval.
3. Compare commanded and measured air changes daily and investigate any divergence.

MAPPINGS

STRIDE	T Tampering, R Repudiation
CAPEC	CAPEC-212 Functionality Misuse
CWE	CWE-306 Missing Authentication for Critical Functionality CWE-862 Missing Authorization
ATT&CK	T0836 Modify Parameter T0832 Manipulation of View T0831 Manipulation of Control
MDS2	AUTH Authorization, AUDT Audit controls
Standards	IEC 62443

CRI-FB-Q Backup power controls disabled

† DIRECT HARM THE HOSPITAL · RANK Q

THREAT

Generator, automatic transfer switch and UPS controllers are reachable from the building network or the internet, often with default credentials. Disabling the transfer or setting generators to manual means the next mains failure, accidental or engineered, takes theatres, ICU and life support down.

MITIGATION PROMPTS (ON THE CARD)

1. Can generator or transfer switch controls be reached from the network?
2. Who would notice if backup power had been set to manual?
3. When was a real changeover to backup power last tested?

MITIGATION PRINCIPLE

Changeover to backup power is protected locally and cannot be disabled from the network.

DESIGN MEASURES

1. Keep transfer and generator start logic local and hardwired, with network access read-only by default.
2. Change default credentials, remove internet exposure and put power controllers in their own segment.
3. Run load tests on a schedule and alarm when any controller leaves automatic mode.

MAPPINGS

STRIDE	D Denial of service, T Tampering
CAPEC	CAPEC-70 Try Common or Default Usernames and Passwords CAPEC-212 Functionality Misuse
CWE	CWE-1392 Use of Default Credentials CWE-306 Missing Authentication for Critical Functionality
ATT&CK	T0816 Device Restart/Shutdown T0837 Loss of Protection T0858 Change Operating Mode
EMB3D	TID-311 Default Credentials
MDS2	SAHD System and application hardening, AUTH Authorization
Standards	IEC 62443

CRI-FB-J Cold storage excursions hidden

† DIRECT HARM THE HOSPITAL · RANK J

THREAT

Blood, vaccine, tissue and pharmacy fridges report to a central temperature monitoring system that can be edited or fed false readings. A heated or failed fridge looks normal, and patients receive spoiled blood products, vaccines or drugs.

MITIGATION PROMPTS (ON THE CARD)

1. How is fridge temperature evidence protected from editing?
2. What independent check confirms blood and vaccines stayed in range?
3. Would a failed fridge still look normal on the central system?

MITIGATION PRINCIPLE

Temperature evidence for stored blood, vaccines and drugs is tamper-evident and checked independently of the monitoring system.

DESIGN MEASURES

1. Use loggers that sign their readings, and keep an independent local display and alarm on each critical unit.
2. Make recorded temperatures read-only after capture and log every acknowledgement and edit.
3. Quarantine stock automatically when readings stop or gaps appear, until a person reviews them.

MAPPINGS

STRIDE	T Tampering, R Repudiation
CAPEC	CAPEC-148 Content Spoofing CAPEC-268 Audit Log Manipulation
CWE	CWE-353 Missing Support for Integrity Check CWE-778 Insufficient Logging
ATT&CK	T0832 Manipulation of View T0838 Modify Alarm Settings
MDS2	IGAU Health data integrity and authenticity, AUDT Audit controls

CRI-FB-10 Water treatment controls changed

† DIRECT HARM THE HOSPITAL · RANK 10

THREAT

Controllers for dialysis water treatment and hot water temperature are networked and maintained remotely. A changed setpoint or silenced quality alarm exposes dialysis patients to contaminated water, or lets Legionella grow in wards where patients are immunocompromised.

MITIGATION PROMPTS (ON THE CARD)

1. What local interlocks protect dialysis water quality?
2. Who can change hot water setpoints remotely?
3. How often does independent testing confirm water quality?

MITIGATION PRINCIPLE

Water quality for dialysis and for vulnerable patients is protected by local interlocks and checked by independent testing.

DESIGN MEASURES

1. Interlock dialysis water production locally so out-of-specification water cannot reach the loop, whatever the network says.
2. Restrict and log setpoint changes on water controllers, and alarm on any change outside a maintenance window.
3. Keep independent sampling and temperature checks on a schedule that does not rely on the control system.

MAPPINGS

STRIDE	T Tampering, D Denial of service
CAPEC	CAPEC-212 Functionality Misuse
CWE	CWE-306 Missing Authentication for Critical Functionality
ATT&CK	T0836 Modify Parameter T0838 Modify Alarm Settings T0880 Loss of Safety
MDS2	AUTH Authorization, AUDT Audit controls
Standards	IEC 62443

CRI-FB-9 Sterilisation cycle records falsified

† DIRECT HARM THE HOSPITAL · RANK 9

THREAT

Washer-disinfectors and autoclaves record cycle parameters to a tracking system that releases instruments. Altered parameters or forged records release unsterile instruments to theatres, or force a recall of every set processed while records cannot be trusted.

MITIGATION PROMPTS (ON THE CARD)

1. What releases instruments: the record, or physical evidence too?
2. Who can change cycle parameters or tracking records?
3. How would you recall sets if cycle records could not be trusted?

MITIGATION PRINCIPLE

Instrument release depends on cycle evidence that cannot be forged and on physical indicators the network cannot change.

DESIGN MEASURES

1. Have sterilisers sign their cycle records and have the tracking system verify them before release.
2. Keep chemical and biological indicators as an independent check on every load.
3. Restrict cycle parameter changes to authenticated engineers, logged and reviewed by sterile services.

MAPPINGS

STRIDE	T Tampering, R Repudiation
CAPEC	CAPEC-148 Content Spoofing
CWE	CWE-353 Missing Support for Integrity Check
ATT&CK	T0836 Modify Parameter T0832 Manipulation of View
MDS2	IGAU Health data integrity and authenticity, AUTH Authorization

CRI-FB-8 Pneumatic tube system stops or misroutes

† CARE DELAYED OR WRONG THE HOSPITAL · RANK 8

THREAT

The pneumatic tube system carries samples, blood and drugs between wards, labs and pharmacy, under one networked controller with embedded stations. Stopping or misrouting it delays results across the hospital, and a compromised station is a foothold on the network.

MITIGATION PROMPTS (ON THE CARD)

1. How would the hospital move samples and drugs without the tube system?
2. What can a tube station reach on the network?
3. Who patches the tube controller and its stations?

SEEN IN PUBLIC

PwnedPiper pneumatic tubes, 2021. Armis disclosed nine vulnerabilities in Swisslog Translogic pneumatic tube system stations, used by thousands of hospitals to move samples and drugs, including unsigned firmware updates that could let an attacker take over stations. Sources: The Register: PwnedPiper flaws in Swisslog pneumatic tube systems; Health-ISAC: Armis discovers 9 vulnerabilities in hospital infrastructure

MITIGATION PRINCIPLE

The tube system's controller and stations are hardened, updated and isolated, and the hospital can run without it.

DESIGN MEASURES

1. Put tube controllers and stations in their own segment with only the connections they need.
2. Require signed firmware for stations and keep them on supported versions.
3. Keep a porter-run courier procedure for urgent samples and blood, and rehearse it.

MAPPINGS

STRIDE	D Denial of service, T Tampering
CAPEC	CAPEC-186 Malicious Software Update
CWE	CWE-494 Download of Code Without Integrity Check CWE-306 Missing Authentication for Critical Functionality
ATT&CK	T0814 Denial of Service T0866 Exploitation of Remote Services
EMB3D	TID-211 Device Allows Unauthenticated Firmware Installation
MDS2	IGAU Health data integrity and authenticity, SAHD System and application hardening

CRI-FB-7 Building management as a pivot

THE HOSPITAL · RANK 7

THREAT

Building management servers and controllers are maintained by contractors, often exposed to the internet, and sit on networks that reach clinical systems. Once inside the building network an attacker moves to device and clinical networks the hospital thought were separate.

MITIGATION PROMPTS (ON THE CARD)

1. What can the building management network reach in the clinical estate?
2. How do contractors connect to building systems remotely?
3. Is any building controller reachable from the internet?

MITIGATION PRINCIPLE

Building systems are a separate zone with controlled conduits, and their remote access is treated like any other privileged access.

DESIGN MEASURES

1. Separate building systems from clinical and corporate networks, allowing only defined, monitored flows between them.
2. Remove internet exposure and route contractor access through the hospital's managed remote access with multi-factor login.
3. Include building controllers in the asset inventory and vulnerability management.

MAPPINGS

STRIDE	E Elevation of privilege, I Information disclosure
CAPEC	CAPEC-700 Network Boundary Bridging
CWE	CWE-923 Improper Restriction of Communication Channel to Intended Endpoints
ATT&CK	T0883 Internet Accessible Device T0866 Exploitation of Remote Services T0822 External Remote Services
MDS2	CONN Connectivity capabilities, RMOT Remote service
Standards	IEC 62443

CRI-FB-6 Infant security and door access defeated

† DIRECT HARM THE HOSPITAL · RANK 6

THREAT

Infant tagging, maternity door locks and access control share controllers and credentials that can be cloned, overridden or disabled. Defeating them enables abduction, and a mass lock or unlock traps people in or opens secure areas during a fire or incident.

MITIGATION PROMPTS (ON THE CARD)

1. Can infant tags or door credentials be cloned or overridden remotely?
2. What do secure doors do in a fire, and in an abduction alert?
3. Who could trigger a mass lock or unlock?

MITIGATION PRINCIPLE

Secure doors fail safe for fire and fail secure for abduction, and their controllers resist cloning and remote override.

DESIGN MEASURES

1. Use access cards that cannot be cloned, and alarm on doors held or forced in maternity and paediatric areas.
2. Make fire release hardwired and local, and log any remote lock or unlock command with who issued it.
3. Test infant tag alarms and door interlocks on a schedule, including when the network is down.

MAPPINGS

STRIDE	S Spoofing, E Elevation of privilege, D Denial of service
LINDDUN	I Identifying
CAPEC	CAPEC-395 Bypassing Electronic Locks and Access Controls CAPEC-390 Bypassing Physical Security
CWE	CWE-1263 Improper Physical Access Control CWE-294 Authentication Bypass by Capture-replay
MDS2	PLOK Physical locks, AUTH Authorization, AUDT Audit controls

CRI-FB-5 Lift priority for patient transfers lost

† CARE DELAYED OR WRONG THE HOSPITAL · RANK 5

THREAT

Lifts that move patients between emergency, theatre and intensive care are run from networked controllers with remote service. Stopping them or removing priority modes delays critical transfers and can trap a patient and team between floors.

MITIGATION PROMPTS (ON THE CARD)

1. Can remote service take patient-transfer lifts out of priority mode?
2. What happens to a patient and team if a lift stops between floors?
3. Who is told before a lift is taken out of service?

MITIGATION PRINCIPLE

Patient-transfer lifts keep their priority and safety functions locally, and remote service cannot take them out of service unannounced.

DESIGN MEASURES

1. Keep firefighter and bed-priority modes under local key control, independent of the network.
2. Restrict remote service to read-only by default and log any command that changes lift mode.
3. Plan alternative transfer routes and staffing for when priority lifts are out of service.

MAPPINGS

STRIDE	D Denial of service
CAPEC	CAPEC-212 Functionality Misuse
CWE	CWE-306 Missing Authentication for Critical Functionality
ATT&CK	T0816 Device Restart/Shutdown T0858 Change Operating Mode
MDS2	RMOT Remote service, AUTH Authorization

CRI-FB-4 Facilities alarms reach nobody

† CARE DELAYED OR WRONG THE HOSPITAL · RANK 4

THREAT

Plant alarms for gases, power, fridges and ventilation are relayed to estates staff by email, SMS or a pager gateway that is unmonitored. When the relay fails, or is overwhelmed by nuisance alarms, a critical alarm sits unread while the plant fails.

MITIGATION PROMPTS (ON THE CARD)

1. Who receives critical plant alarms, and must they acknowledge them?
2. What tells estates staff that the alarm relay has failed?
3. How many nuisance alarms bury the critical ones?

MITIGATION PRINCIPLE

Critical facilities alarms reach a person who acknowledges them, and failure of the relay is itself an alarm.

DESIGN MEASURES

1. Require acknowledgement of critical alarms and escalate automatically when none arrives in time.
2. Send a heartbeat through the alarm relay and alarm locally when it stops.
3. Review alarm volumes monthly and remove nuisance alarms so critical ones stand out.

MAPPINGS

STRIDE	D Denial of service
CAPEC	CAPEC-607 Obstruction
CWE	CWE-1320 Improper Protection for Outbound Error Messages and Alert Signals CWE-754 Improper Check for Unusual or Exceptional Conditions
ATT&CK	T0878 Alarm Suppression
MDS2	CONN Connectivity capabilities

CRI-FB-3 Engineering drawings and asset data exposed

THE HOSPITAL · RANK 3

THREAT

Drawings of gas, power and ventilation systems, asset registers and controller addresses are shared in tenders, contractor portals and project files. They tell an attacker exactly which controller feeds which theatre or ward.

MITIGATION PROMPTS (ON THE CARD)

1. Where are drawings of gas, power and ventilation shared?
2. Who can see which controller feeds which theatre?
3. Is access to engineering information tracked and limited?

MITIGATION PRINCIPLE

Engineering information about critical building systems is shared on a need-to-know basis and tracked.

DESIGN MEASURES

1. Classify engineering drawings and asset data, and share them only through controlled portals with named access.
2. Remove controller addresses and credentials from tender and handover documents.
3. Require contractors to return or destroy engineering information at the end of a project.

MAPPINGS

STRIDE	I Information disclosure
CAPEC	CAPEC-169 Footprinting CAPEC-406 Dumpster Diving
CWE	CWE-552 Files or Directories Accessible to External Parties
ATT&CK	T0882 Theft of Operational Information
MDS2	MPII Management of private data

CRI-FB-2 Energy optimisation darkens clinical areas

THE HOSPITAL · RANK 2

THREAT

Energy and lighting optimisation schedules, set centrally or by a vendor platform, apply office logic to clinical areas. A changed schedule switches off lighting, ventilation or heating in a ward, theatre or recovery area overnight.

MITIGATION PROMPTS (ON THE CARD)

1. Which clinical areas do automated energy schedules touch?
2. Who approves an energy rule that affects a ward or theatre?
3. Could a vendor platform change lighting or ventilation overnight?

MITIGATION PRINCIPLE

Clinical areas are excluded from automated energy schedules unless clinicians have approved the rule.

DESIGN MEASURES

1. Tag clinical zones in the building system and block energy rules from applying to them by default.
2. Log and review every schedule change, including those pushed by the vendor platform.
3. Give each clinical area a local override that restores lighting and ventilation immediately.

MAPPINGS

STRIDE	T Tampering, D Denial of service
CAPEC	CAPEC-212 Functionality Misuse
CWE	CWE-1188 Initialization of a Resource with an Insecure Default
ATT&CK	T0836 Modify Parameter
MDS2	AUTH Authorization

CRI-SV · THE HOSPITAL · 13 ENTRIES

Suppliers, Service and Lifecycle

Vendor remote service, service laptops, manufacturer clouds, patching rights, end of support, procurement evidence, refurbished devices, disposal and vendor failure.

https://ostering.com/taxonomies/hospitals-and-medical-devices/suppliers-service-and-lifecycle/

CRI-SV-A One service password, every hospital

† DIRECT HARM THE HOSPITAL · RANK A

THREAT

A manufacturer uses the same service password, key or certificate on every unit it ships, and its engineers know it. Once it leaks, anyone can reach service functions on that model in every hospital at once, and the hospitals cannot change it.

MITIGATION PROMPTS (ON THE CARD)

1. Is any service credential shared across every unit of this model?
2. Can the hospital change service credentials without the vendor?
3. What would one leaked service password open across your sites?

MITIGATION PRINCIPLE

Service credentials are unique per device, owned by the hospital, and changeable without the vendor.

DESIGN MEASURES

1. Require unique per-device service credentials at procurement, and refuse devices with shared or hard-coded ones.
2. Let the hospital rotate service credentials and issue them to engineers for a visit, logged.
3. Ask vendors to confirm in writing how service credentials are generated, stored and revoked.

MAPPINGS

STRIDE	S Spoofing, E Elevation of privilege
CAPEC	CAPEC-70 Try Common or Default Usernames and Passwords CAPEC-191 Read Sensitive Constants Within an Executable
CWE	CWE-798 Use of Hard-coded Credentials CWE-1273 Device Unlock Credential Sharing
ATT&CK	T1078.001 Default Accounts T1199 Trusted Relationship
EMB3D	TID-328 Hardcoded Credentials TID-311 Default Credentials
MDS2	PAUT Person authentication, RMOT Remote service, AUTH Authorization
Standards	FDA premarket IEC 81001-5-1

CRI-SV-K Always-on vendor remote service

† CARE DELAYED OR WRONG THE HOSPITAL · RANK K

THREAT

Vendors keep permanent tunnels, modems or remote-access tools into their devices for service, outside the hospital's control. Compromise of the vendor, or of one technician, opens a path into many hospitals' device networks at once.

MITIGATION PROMPTS (ON THE CARD)

1. Which vendors hold permanent remote access into devices?
2. Who approves each remote service session, and is it recorded?
3. How would you know a vendor tunnel had been misused?

MITIGATION PRINCIPLE

Vendor remote access is brokered, approved per session, recorded, and closed when the work ends.

DESIGN MEASURES

1. Route all vendor access through the hospital's managed access service with multi-factor login and per-session approval.
2. Remove cellular modems and vendor-installed remote tools that bypass the hospital's controls.
3. Record sessions and review them against the service ticket.

MAPPINGS

STRIDE	S Spoofing, E Elevation of privilege
CAPEC	CAPEC-555 Remote Services with Stolen Credentials
CWE	CWE-923 Improper Restriction of Communication Channel to Intended Endpoints
ATT&CK	T1133 External Remote Services T1199 Trusted Relationship T1219 Remote Access Tools
MDS2	RMOT Remote service, AUDT Audit controls
Standards	IEC 80001-1

CRI-SV-Q Care depends on the vendor's cloud

† CARE DELAYED OR WRONG THE HOSPITAL · RANK Q

THREAT

Treatment planning, device configuration, remote follow-up or reporting run in the manufacturer's cloud. A ransomware attack or outage there stops care at every customer at once, and hospitals have no local fallback.

MITIGATION PROMPTS (ON THE CARD)

1. Which clinical functions stop if the vendor's cloud is down?
2. What degraded mode keeps care running locally?
3. When was a vendor cloud outage last rehearsed?

SEEN IN PUBLIC

Elekta cloud outage, 2021. Ransomware hit Elekta's first-generation US cloud service for radiation oncology software, and about 170 US health systems were affected; some cancer centres could not treat patients for over a week because treatment programming was held in the cloud. Sources: Compliancy Group: Healthcare vendor ransomware attack, 170 health systems hit; Yale Daily News: YNHHS pauses radiotherapy treatment for six days

MITIGATION PRINCIPLE

Clinically essential functions keep working, at least in a degraded mode, when the vendor's cloud is unavailable.

DESIGN MEASURES

1. Identify which clinical functions need the vendor cloud and require a documented local fallback for each.
2. Keep local copies of plans, configurations and data needed to treat current patients.
3. Include the vendor's incident notification and recovery commitments in the contract and exercise them.

MAPPINGS

STRIDE	D Denial of service
CWE	CWE-1357 Reliance on Insufficiently Trustworthy Component
ATT&CK	T1489 Service Stop
MDS2	DTBK Data backup and disaster recovery, RDMP Roadmap for third-party components
Standards	IEC 80001-1

CRI-SV-J End of support with no exit

† CARE DELAYED OR WRONG THE HOSPITAL · RANK J

THREAT

Devices run operating systems and components the manufacturer no longer supports, and replacement is unaffordable or years away. Known vulnerabilities stay open in clinical use, and one worm can take out imaging, lab and monitoring together.

MITIGATION PROMPTS (ON THE CARD)

1. Which devices are past their manufacturer's end of support?
2. How are unsupported devices isolated until replacement?
3. When is each unsupported device due to be replaced?

SEEN IN PUBLIC

WannaCry and the NHS, 2017. WannaCry ransomware disrupted at least 81 of England's 236 NHS trusts and infected 595 GP practices; the NAO estimated over 19,000 appointments were cancelled, and some trusts diverted ambulances. Sources: NAO: Investigation, WannaCry cyber attack and the NHS; GOV.UK: Foreign Office Minister condemns North Korean actor for WannaCry attacks

MITIGATION PRINCIPLE

Every device has a planned end of support, and devices past it are isolated and scheduled for replacement.

DESIGN MEASURES

1. Record end-of-support dates for each device and its third-party components at purchase.
2. Isolate unsupported devices in restricted segments with only the flows they need.
3. Budget replacement cycles from end-of-support dates, and report the unsupported estate to the board.

MAPPINGS

STRIDE	T Tampering, D Denial of service
CAPEC	CAPEC-310 Scanning for Vulnerable Software
CWE	CWE-1104 Use of Unmaintained Third Party Components CWE-1329 Reliance on Component That is Not Updateable
ATT&CK	T1210 Exploitation of Remote Services
EMB3D	TID-210 Device Vulnerabilities Unpatchable
MDS2	RDMP Roadmap for third-party components, SAHD System and application hardening
Standards	AAMI SW96 IEC 80001-1

CRI-SV-10 Only the vendor may patch

† CARE DELAYED OR WRONG THE HOSPITAL · RANK 10

THREAT

Hospitals are not allowed to patch validated devices, and manufacturers take months to validate updates, often without saying what to do meanwhile. Known exploited vulnerabilities stay open, and staff patch anyway and break the device's validated state.

MITIGATION PROMPTS (ON THE CARD)

1. What timeline has the vendor committed to for validated updates?
2. Which interim mitigations can the hospital apply safely?
3. What happens when staff patch a validated device themselves?

MITIGATION PRINCIPLE

Manufacturers commit to timelines for validated updates and give interim mitigations the hospital can apply safely.

DESIGN MEASURES

1. Contract for maximum times to validated security updates and for interim compensating controls.
2. Ask for a list of operating system patches the hospital may apply without revalidation.
3. Track each open vulnerability on clinical devices with its mitigation and review date.

MAPPINGS

STRIDE	T Tampering, D Denial of service
CWE	CWE-1329 Reliance on Component That is Not Updateable CWE-671 Lack of Administrator Control over Security
ATT&CK	T1210 Exploitation of Remote Services
EMB3D	TID-210 Device Vulnerabilities Unpatchable
MDS2	CSUP Cybersecurity product upgrades, SGUD Security guidance
Standards	AAMI SW96 FDA premarket

CRI-SV-9 Service laptops carry infection between hospitals

† CARE DELAYED OR WRONG THE HOSPITAL · RANK 9

THREAT

Field engineers plug their laptops and USB drives into devices at hospital after hospital, using service software with full control. Malware or a tampered tool spreads from one site to the next and onto devices the hospital's protections never see.

MITIGATION PROMPTS (ON THE CARD)

1. How are service laptops and USB drives checked before touching a device?
2. Who records which tools were used on which device?
3. Could malware travel on an engineer's kit from another hospital?

MITIGATION PRINCIPLE

Service tools and media are treated as transient assets: checked, controlled and recorded before they touch a device.

DESIGN MEASURES

1. Scan engineers' laptops and media at a kiosk before connection, and record the asset used.
2. Offer hospital-owned service workstations for vendors where devices allow it.
3. Require vendors to describe how service laptops are managed, patched and protected.

MAPPINGS

STRIDE	T Tampering, E Elevation of privilege
CAPEC	CAPEC-457 USB Memory Attacks
CWE	CWE-829 Inclusion of Functionality from Untrusted Control Sphere
ATT&CK	T1091 Replication Through Removable Media T0864 Transient Cyber Asset
EMB3D	TID-303 Excessive Trust in Offboard Management/IDE Software
MDS2	MLDP Malware detection and protection, RMOT Remote service
Standards	IEC 80001-1

CRI-SV-8 Update channel delivers malicious updates

† DIRECT HARM THE HOSPITAL · RANK 8

THREAT

Device and software updates arrive from the vendor's portal, a service engineer or a distribution server, and devices accept what they are given. A compromised vendor or update server pushes tampered firmware or software across the installed base.

MITIGATION PROMPTS (ON THE CARD)

1. Does each device verify updates itself, whatever the delivery route?
2. Which servers and people can deliver updates to devices?
3. How many devices would one tampered update reach?

MITIGATION PRINCIPLE

Devices accept only updates signed by the manufacturer and verify them themselves, whatever the delivery route.

DESIGN MEASURES

1. Require signed updates verified on the device, with rollback protection.
2. Verify update packages against published hashes before staging them in the hospital.
3. Stage updates on a sample of devices and watch for unexpected behaviour before wider rollout.

MAPPINGS

STRIDE	T Tampering, E Elevation of privilege
CAPEC	CAPEC-186 Malicious Software Update CAPEC-669 Alteration of a Software Update
CWE	CWE-494 Download of Code Without Integrity Check CWE-347 Improper Verification of Cryptographic Signature
ATT&CK	T1195.002 Compromise Software Supply Chain
EMB3D	TID-211 Device Allows Unauthenticated Firmware Installation TID-213 Faulty FW/SW Update Integrity Verification TID-216 Firmware Update Rollbacks Allowed
MDS2	IGAU Health data integrity and authenticity, CSUP Cybersecurity product upgrades
Standards	FDA premarket IEC 81001-5-1

CRI-SV-7 Bought without security evidence

THE HOSPITAL · RANK 7

THREAT

Devices and clinical systems are bought on clinical and price criteria alone, without a security disclosure, SBOM, support period or vulnerability handling commitment. Once installed, the weaknesses cannot be bought back.

MITIGATION PROMPTS (ON THE CARD)

1. Is security evidence scored alongside clinical criteria at purchase?
2. Did the supplier commit to a support period and vulnerability handling?
3. Which installed systems were bought without an SBOM?

MITIGATION PRINCIPLE

Security evidence and lifecycle commitments are procurement criteria with the same weight as clinical ones.

DESIGN MEASURES

1. Require an MDS2, an SBOM, a support end date and a disclosure process in every tender.
2. Include clinical engineering and security in evaluation, with the power to fail a bid.
3. Write security update and notification obligations into the contract.

MAPPINGS

STRIDE	T Tampering, I Information disclosure, D Denial of service
CWE	CWE-1357 Reliance on Insufficiently Trustworthy Component
MDS2	SBOM Software bill of materials, RDMP Roadmap for third-party components, SGUD Security guidance
Standards	IEC 80001-1 AAMI SW96

CRI-SV-6 Refurbished and grey-market devices

† DIRECT HARM THE HOSPITAL · RANK 6

THREAT

Refurbished, loaned and grey-market devices arrive with unknown firmware, counterfeit parts, another hospital's configuration and sometimes its patients' data. They can behave unpredictably and carry weaknesses or implants nobody checked for.

MITIGATION PROMPTS (ON THE CARD)

1. How is a refurbished or loaned device restored to a known state?
2. Who verifies a second-hand device's origin and firmware?
3. Could a device arrive holding another hospital's patients or settings?

MITIGATION PRINCIPLE

Every device entering service is restored to a known configuration and its origin and firmware are verified.

DESIGN MEASURES

1. Buy refurbished devices only through manufacturer-authorised channels with documented provenance.
2. Reset devices to factory configuration and verify firmware versions and hashes before clinical use.
3. Check incoming devices for previous owners' data and network credentials, and remove them.

MAPPINGS

STRIDE	T Tampering, I Information disclosure
LINDDUN	DD Data disclosure
CAPEC	CAPEC-535 Malicious Gray Market Hardware CAPEC-530 Provide Counterfeit Component
CWE	CWE-1357 Reliance on Insufficiently Trustworthy Component CWE-226 Sensitive Information in Resource Not Removed Before Reuse
ATT&CK	T1195.003 Compromise Hardware Supply Chain
EMB3D	TID-113 Unverified Peripheral Firmware Loaded
MDS2	IGAU Health data integrity and authenticity, MPII Management of private data

CRI-SV-5 Disposed devices leak patients and passwords

THE HOSPITAL · RANK 5

THREAT

Devices returned to the vendor, sold or scrapped still hold patient data, network keys and service credentials. Anyone who buys them on the second-hand market can read the data and use the keys to get onto the hospital's network.

MITIGATION PROMPTS (ON THE CARD)

1. What standard is used to sanitise devices before they leave?
2. Which credentials does a disposed device hold that need rotating?
3. Who records that sanitisation actually happened?

MITIGATION PRINCIPLE

Every device leaving the hospital is sanitised to a recorded standard, and credentials it held are rotated.

DESIGN MEASURES

1. Wipe or destroy storage in every departing device using a method the manufacturer confirms, and keep a certificate.
2. Rotate Wi-Fi keys, certificates and accounts the device held when it leaves service.
3. Require vendors taking devices back to sanitise them and confirm it in writing.

MAPPINGS

STRIDE	I Information disclosure
LINDDUN	DD Data disclosure, I Identifying
CAPEC	CAPEC-675 Retrieve Data from Decommissioned Devices
CWE	CWE-1266 Improper Scrubbing of Sensitive Data from Decommissioned Device CWE-226 Sensitive Information in Resource Not Removed Before Reuse
ATT&CK	T1052 Exfiltration Over Physical Medium
EMB3D	TID-108 ROM/NVRAM Data Extraction or Modification
MDS2	MPII Management of private data, STCF Data storage confidentiality, DIDT Health data de-identification
Standards	ISO 27799

CRI-SV-4 Vendor collapses or changes hands

† CARE DELAYED OR WRONG THE HOSPITAL · RANK 4

THREAT

A manufacturer goes bust, withdraws a product or is acquired, and support, cloud services, signing keys and spare parts go with it. Hospitals and patients are left with devices nobody can update, service or safely replace.

MITIGATION PROMPTS (ON THE CARD)

1. What happens to support, keys and spares if the vendor fails?
2. Does the contract cover a change of ownership?
3. Which devices depend on one vendor's continued existence?

SEEN IN PUBLIC

Argus II retinal implant, 2020. Second Sight phased out its Argus II retinal implant and, after laying off most staff in March 2020, could no longer support its more than 350 recipients; patients were left with implants that could not be repaired and, in one case, could not get an MRI without the maker's input. Sources: IEEE Spectrum: Their bionic eyes are now obsolete and unsupported

MITIGATION PRINCIPLE

Hospitals plan for losing a supplier and contract for what happens to support, keys and data if they do.

DESIGN MEASURES

1. Contract for escrow of documentation, service tools and update capability if the vendor exits the market.
2. Identify single-supplier devices and plan alternatives before they are needed.
3. Require notice of product withdrawal and a support period after it.

MAPPINGS

STRIDE	D Denial of service
CWE	CWE-1329 Reliance on Component That is Not Updateable
MDS2	RDMP Roadmap for third-party components
Standards	AAMI SW96

CRI-SV-3 No SBOM, no answer

THE HOSPITAL · RANK 3

THREAT

When a vulnerability is announced in a common component, the hospital cannot tell which of its devices contain it, and the vendor takes weeks to say. Exposure is unknown while attackers already know where to look.

MITIGATION PROMPTS (ON THE CARD)

1. Can you match a new component vulnerability to your devices in hours?
2. Which devices have no current component list?
3. How quickly do vendors answer exposure questions?

SEEN IN PUBLIC

URGENT/11, 2019. The FDA warned that 11 vulnerabilities in IPnet, a third-party network stack inside several embedded operating systems, could let attackers take over or crash medical devices and hospital network equipment, and that manufacturers might not know their products contained it. Sources: Healthcare IT News: URGENT/11, FDA issues alert

SweynTooth Bluetooth flaws, 2020. The FDA warned that SweynTooth flaws in Bluetooth Low Energy chips used in pacemakers, glucose monitors, insulin pumps and other devices could let someone nearby crash a device, stop it working or bypass security. Sources: RAPS: FDA warns of cybersecurity vulnerabilities in pacemakers and other BLE devices; HPN: FDA informs about potential vulnerabilities in medical devices with Bluetooth Low Energy

MITIGATION PRINCIPLE

Hospitals hold current component lists for their devices and can match a new vulnerability to devices in hours.

DESIGN MEASURES

1. Require machine-readable SBOMs at purchase and with every update.
2. Load SBOMs into the asset inventory and match them automatically against new vulnerability notices.
3. Ask vendors for exploitability statements so effort goes where it matters.

MAPPINGS

STRIDE	I Information disclosure
CWE	CWE-1395 Dependency on Vulnerable Third-Party Component CWE-1104 Use of Unmaintained Third Party Components
EMB3D	TID-202 Exploitable System Network Stack Component
MDS2	SBOM Software bill of materials, RDMP Roadmap for third-party components
Standards	FDA premarket IEC 81001-5-1

CRI-SV-2 Advisories never reach the ward

THE HOSPITAL · RANK 2

THREAT

Manufacturers' security notices go to a sales or procurement contact, not to clinical engineering, and hospitals have no published way to report problems. Fixes and warnings sit in an inbox while vulnerable devices stay in use.

MITIGATION PROMPTS (ON THE CARD)

1. Who at the hospital receives manufacturers' security advisories?
2. How does the hospital report a problem to a vendor?
3. How long does an advisory take to reach clinical engineering?

MITIGATION PRINCIPLE

Security advisories have a named destination on both sides, and the hospital can report problems to the vendor.

DESIGN MEASURES

1. Register a monitored security contact with every device vendor and keep it current.
2. Require vendors to run a coordinated vulnerability disclosure process and say how they notify customers.
3. Route advisories to clinical engineering and track each to closure.

MAPPINGS

STRIDE	I Information disclosure
CWE	CWE-1357 Reliance on Insufficiently Trustworthy Component
MDS2	SGUD Security guidance, CSUP Cybersecurity product upgrades
Standards	AAMI SW96

CRI-AC · THE HOSPITAL · 13 ENTRIES

Identity and Access

Clinician identities, default and hard-coded credentials, shared directories, shared logins, break-glass, session handover, privileged and temporary accounts, badges.

https://ostering.com/taxonomies/hospitals-and-medical-devices/identity-and-access/

CRI-AC-A Stolen clinician identity prescribes and signs

† CARE DELAYED OR WRONG THE HOSPITAL · RANK A

THREAT

A clinician's account can prescribe, sign results, discharge patients and change care plans from any workstation or remote session, with no stronger check for high-risk actions. A phished or reused password lets an attacker order, cancel or approve care under a trusted name.

MITIGATION PROMPTS (ON THE CARD)

1. Which clinical actions need stronger proof than reading a record?
2. How are remote clinical sessions authenticated?
3. Who is told when orders appear under a clinician's name unusually?

MITIGATION PRINCIPLE

High-risk clinical actions need stronger proof of who is acting than reading a record does.

DESIGN MEASURES

1. Require step-up authentication, such as a smartcard tap or a second factor, for prescribing, signing results and changing allergies.
2. Bind remote and off-site clinical sessions to managed devices and phishing-resistant authentication.
3. Alert the clinician and their lead when orders are placed under their name from an unusual place or time.

MAPPINGS

STRIDE	S Spoofing, E Elevation of privilege, R Repudiation
CAPEC	CAPEC-560 Use of Known Domain Credentials CAPEC-98 Phishing
CWE	CWE-308 Use of Single-factor Authentication
ATT&CK	T1078 Valid Accounts T1566 Phishing
MDS2	PAUT Person authentication, AUTH Authorization, AUDT Audit controls
Standards	ISO 27799

CRI-AC-K Default and hard-coded device credentials

† DIRECT HARM THE HOSPITAL · RANK K

THREAT

Devices ship with default administrator passwords that nobody changes, or with credentials compiled into the firmware that cannot be changed. Anyone on the clinical network can log in and change settings, alarm limits or therapy, and the hospital has no way to close the door short of replacing the device.

MITIGATION PROMPTS (ON THE CARD)

1. Which devices still use default or hard-coded credentials?
2. Can the hospital set and change every device credential?
3. What could someone on the clinical network change with a default password?

MITIGATION PRINCIPLE

No device should be reachable with a credential the hospital did not set and cannot change.

DESIGN MEASURES

1. Force a unique credential to be set at installation before the device will run clinically.
2. Remove hard-coded accounts; where an account must exist, make it changeable and disable it by default.
3. Ask for default and hard-coded credentials in procurement (MDS2) and reject devices that cannot answer.

MAPPINGS

STRIDE	S Spoofing, T Tampering, E Elevation of privilege
CAPEC	CAPEC-70 Try Common or Default Usernames and Passwords CAPEC-115 Authentication Bypass
CWE	CWE-1393 Use of Default Password CWE-259 Use of Hard-coded Password CWE-798 Use of Hard-coded Credentials
ATT&CK	T1078.001 Default Accounts T0859 Valid Accounts
EMB3D	TID-311 Default Credentials TID-328 Hardcoded Credentials
MDS2	PAUT Person authentication, SAHD System and application hardening, AUTH Authorization
Standards	IEC 81001-5-1 IEC TR 60601-4-5 FDA premarket

CRI-AC-Q One directory for IT and devices

† CARE DELAYED OR WRONG THE HOSPITAL · RANK Q

THREAT

Modality workstations, monitoring servers, lab middleware and pharmacy systems all join the same directory as office PCs. One stolen administrator account or one domain compromise reaches every clinical system at once, and ransomware spreads to the devices along with the desktops.

MITIGATION PROMPTS (ON THE CARD)

1. Which clinical systems join the same directory as office PCs?
2. What would one stolen domain administrator account reach?
3. Could clinical devices keep running if the directory were lost?

SEEN IN PUBLIC

WannaCry and the NHS, 2017. WannaCry ransomware disrupted at least 81 of England's 236 NHS trusts and infected 595 GP practices; the NAO estimated over 19,000 appointments were cancelled, and some trusts diverted ambulances. Sources: NAO: Investigation, WannaCry cyber attack and the NHS; GOV.UK: Foreign Office Minister condemns North Korean actor for WannaCry attacks

Conti attack on Ireland's HSE, 2021. Conti ransomware encrypted about 80% of the Health Service Executive's IT environment and about 700 GB of data was taken; the HSE shut its national IT down and took around four months to recover fully. PwC's independent post-incident review was published in December 2021. Sources: HSE: Conti cyber attack on the HSE, full report (PwC); HHS HC3: Lessons learned from the HSE cyber attack

MITIGATION PRINCIPLE

A compromise of the corporate identity system must not hand over the clinical device estate.

DESIGN MEASURES

1. Run clinical device systems in a separate identity domain with no trust from the corporate directory.
2. Use separate administrator accounts and workstations for the device estate, never reused for email or browsing.
3. Test that a fully compromised corporate domain cannot log in to any device or clinical server.

MAPPINGS

STRIDE	S Spoofing, E Elevation of privilege, D Denial of service
CAPEC	CAPEC-560 Use of Known Domain Credentials CAPEC-652 Use of Known Kerberos Credentials CAPEC-509 Kerberoasting
CWE	CWE-266 Incorrect Privilege Assignment CWE-1220 Insufficient Granularity of Access Control
ATT&CK	T1078.002 Domain Accounts T1021.002 SMB/Windows Admin Shares T1486 Data Encrypted for Impact
MDS2	AUTH Authorization, SAHD System and application hardening
Standards	IEC 80001-1 IEC 62443

CRI-AC-J Devices without their own identity

† CARE DELAYED OR WRONG THE HOSPITAL · RANK J

THREAT

Systems accept vital signs, results or images from anything on the network that speaks the right protocol. A rogue or spoofed node can pose as a monitor, analyser or modality and write false values into the record, which clinicians then act on.

MITIGATION PROMPTS (ON THE CARD)

1. How does a receiving system know which device sent the data?
2. What happens to data from an unknown or spoofed node?
3. Could a rogue device pose as a monitor or analyser?

MITIGATION PRINCIPLE

Every device that writes clinical data proves which device it is, and the receiver refuses data from unknown sources.

DESIGN MEASURES

1. Give each device a certificate or key at installation and require mutual authentication to gateways and interfaces.
2. Keep a register of devices allowed to send to each interface and reject the rest.
3. Alert clinical engineering when a new or unexpected source appears on a clinical feed.

MAPPINGS

STRIDE	S Spoofing, T Tampering
CAPEC	CAPEC-151 Identity Spoofing CAPEC-194 Fake the Source of Data
CWE	CWE-306 Missing Authentication for Critical Functionality CWE-924 Improper Enforcement of Message Integrity During Transmission in a Communication Channel
ATT&CK	T1565.002 Transmitted Data Manipulation
EMB3D	TID-406 Unauthorized Messages or Connections
MDS2	NAUT Node authentication, IGAU Health data integrity and authenticity
Standards	IEC 80001-1 IEC 81001-5-1

CRI-AC-10 Help-desk resets for urgent callers

THE HOSPITAL · RANK 10

THREAT

The service desk resets passwords and multi-factor enrolment for anyone who sounds like a busy consultant with a patient waiting. An attacker who knows names and rotas from public pages gets a clinician's or administrator's access in one phone call.

MITIGATION PROMPTS (ON THE CARD)

1. How does the service desk prove a caller's identity?
2. Are privileged resets harder than ordinary ones?
3. What public information would help an attacker sound convincing?

MITIGATION PRINCIPLE

Urgency must never replace identity proofing for credential resets, and resets must be harder for privileged accounts.

DESIGN MEASURES

1. Verify callers through a second channel or in person before any reset, with a fast route for genuine emergencies.
2. Require a manager or second approver for resets of privileged and remote-access accounts.
3. Notify the account owner on every reset and enrolment change, through a channel the caller does not control.

MAPPINGS

STRIDE	S Spoofing, E Elevation of privilege
CAPEC	CAPEC-407 Pretexting CAPEC-416 Manipulate Human Behavior
CWE	CWE-640 Weak Password Recovery Mechanism for Forgotten Password
ATT&CK	T1566.004 Spearphishing Voice T1098.005 Device Registration T1078 Valid Accounts
MDS2	PAUT Person authentication, AUTH Authorization
Standards	ISO 27799

CRI-AC-9 Break-glass becomes the normal route

THE HOSPITAL · RANK 9

THREAT

Emergency access to records and devices is so easy, or normal access so slow, that staff use break-glass every shift. Nobody reviews it, so snooping on records and unattributed changes hide in the noise, and the control meant for emergencies stops meaning anything.

MITIGATION PROMPTS (ON THE CARD)

1. How often is break-glass used, and why so often?
2. Who reviews each break-glass use, and how quickly?
3. Is normal access slow enough to push staff to emergency access?

MITIGATION PRINCIPLE

Emergency access is quick in an emergency, rare in practice and reviewed every time it is used.

DESIGN MEASURES

1. Fix the routine access problems that drive break-glass use before adding more controls.
2. Ask for a reason at break-glass and send every use to a reviewer within a day.
3. Report break-glass rates by ward and role so routine use is visible and challenged.

MAPPINGS

STRIDE	R Repudiation, I Information disclosure, E Elevation of privilege
LINDDUN	Nr Non-repudiation, DD Data disclosure, Nc Non-compliance
CAPEC	CAPEC-122 Privilege Abuse
CWE	CWE-778 Insufficient Logging CWE-863 Incorrect Authorization
ATT&CK	T1078 Valid Accounts
MDS2	EMRG Emergency access, AUDT Audit controls
Standards	ISO 27799 IEC 80001-1

CRI-AC-8 Generic and shared clinical logins

THE HOSPITAL · RANK 8

THREAT

Wards share generic accounts on workstations, devices and departmental systems because individual logins are too slow. Orders, results, settings and record views cannot be tied to a person, so mistakes and misuse go uninvestigated and leavers keep access through the shared password.

MITIGATION PROMPTS (ON THE CARD)

1. Which wards or devices still rely on generic accounts?
2. Can every order and setting change be tied to a person?
3. What would make individual login as fast as the shared one?

MITIGATION PRINCIPLE

Every clinical action is attributable to a person, without making shared devices slower to use.

DESIGN MEASURES

1. Replace generic accounts with fast individual sign-on, such as badge tap with a short PIN.
2. Where a device must run under a shared account, record who is signed in to the session alongside it.
3. Change shared passwords whenever a holder leaves and audit for generic account use on clinical systems.

MAPPINGS

STRIDE	S Spoofing, R Repudiation
LINDDUN	Nr Non-repudiation
CAPEC	CAPEC-21 Exploitation of Trusted Identifiers
CWE	CWE-286 Incorrect User Management CWE-1220 Insufficient Granularity of Access Control
ATT&CK	T1078.003 Local Accounts
MDS2	PAUT Person authentication, AUDT Audit controls
Standards	ISO 27799

CRI-AC-7 Session handed to the next user

† CARE DELAYED OR WRONG THE HOSPITAL · RANK 7

THREAT

Shared workstations on wheels and bedside terminals stay signed in as the last person. The next clinician prescribes, records or views under someone else's name, sometimes on the wrong patient's open record, and the record shows the wrong author for clinical decisions.

MITIGATION PROMPTS (ON THE CARD)

1. Does the shared screen always show who is signed in?
2. How quickly can the next clinician switch user?
3. Could someone prescribe on the wrong patient's open record?

MITIGATION PRINCIPLE

A shared screen always shows who is signed in and which patient is open, and switches user quickly and safely.

DESIGN MEASURES

1. Use fast user switching that closes the previous user's patient context.
2. Show the signed-in user and patient prominently on every clinical screen.
3. Lock idle sessions on a timeout suited to the area, shorter in public areas than in theatres.

MAPPINGS

STRIDE	S Spoofing, R Repudiation
LINDDUN	Nr Non-repudiation
CAPEC	CAPEC-593 Session Hijacking CAPEC-60 Reusing Session IDs (aka Session Replay)
CWE	CWE-1463 Insufficient Session Timeout Value CWE-1464 Improper Session Invalidation
MDS2	ALOF Automatic logoff, PAUT Person authentication
Standards	ISO 27799

CRI-AC-6 Standing privilege for biomed and IT

† CARE DELAYED OR WRONG THE HOSPITAL · RANK 6

THREAT

Clinical engineering and IT staff hold permanent administrator rights to every device console, monitoring server and integration engine. One phished or reused account gives an attacker the power to change any device or interface in the hospital, with nothing to approve or notice.

MITIGATION PROMPTS (ON THE CARD)

1. Which biomed and IT accounts hold standing administrator rights?
2. Is privilege granted for a task and seen by someone else?
3. What could one phished engineer account change?

MITIGATION PRINCIPLE

Privilege over clinical systems is granted for a task, for a time, and is seen by someone else.

DESIGN MEASURES

1. Grant device and integration admin rights just in time, with approval and expiry.
2. Use phishing-resistant authentication for every privileged clinical account.
3. Alert on privileged changes to device settings, alarm limits and interface routes outside change windows.

MAPPINGS

STRIDE	E Elevation of privilege, R Repudiation
CAPEC	CAPEC-122 Privilege Abuse CAPEC-233 Privilege Escalation
CWE	CWE-250 Execution with Unnecessary Privileges CWE-266 Incorrect Privilege Assignment
ATT&CK	T1078 Valid Accounts T1098.007 Additional Local or Domain Groups
MDS2	AUTH Authorization, AUDT Audit controls, PAUT Person authentication
Standards	IEC 80001-1 IEC 62443

CRI-AC-5 Agency, locum and leaver accounts

THE HOSPITAL · RANK 5

THREAT

Agency nurses, locum doctors, students and contractors get accounts in a hurry and nobody removes them. Accounts outlive the people, are shared between shifts or reach remote access, giving former staff and anyone who buys their password a way into records and systems.

MITIGATION PROMPTS (ON THE CARD)

1. Who sponsors each agency, locum and contractor account?
2. Does every temporary account have an end date?
3. How quickly is access removed when someone leaves?

MITIGATION PRINCIPLE

Every account has an owner, an end date and a sponsor who answers for it.

DESIGN MEASURES

1. Give temporary staff accounts an end date at creation and require a sponsor to extend them.
2. Feed starters and leavers from rostering and HR into account removal automatically.
3. Review dormant and remote-capable accounts monthly and disable those unused for a set period.

MAPPINGS

STRIDE	S Spoofing, E Elevation of privilege
LINDDUN	I Identifying
CAPEC	CAPEC-560 Use of Known Domain Credentials
CWE	CWE-286 Incorrect User Management
ATT&CK	T1078 Valid Accounts T1133 External Remote Services
MDS2	AUTH Authorization, PAUT Person authentication
Standards	ISO 27799

CRI-AC-4 Authentication friction drives workarounds

† CARE DELAYED OR WRONG THE HOSPITAL · RANK 4

THREAT

Logins and multi-factor prompts that take too long in a resuscitation or theatre push staff to write passwords on monitors, share tokens, prop sessions open or disable locks. The workaround becomes the real control, and both security and care suffer.

MITIGATION PROMPTS (ON THE CARD)

1. How many seconds does login take in resuscitation or theatre?
2. Which workarounds do staff use when authentication is slow?
3. Were clinicians involved in testing the authentication design?

MITIGATION PRINCIPLE

Authentication is designed around clinical workflow, measured in seconds, and tested with clinicians.

DESIGN MEASURES

1. Time sign-in and switch-user on real wards and set a target in seconds.
2. Use proximity or badge tap with risk-based step-up rather than repeated full logins.
3. Watch for workarounds such as written passwords and fix the cause, not the person.

MAPPINGS

STRIDE	S Spoofing, E Elevation of privilege
CAPEC	CAPEC-416 Manipulate Human Behavior
CWE	CWE-655 Insufficient Psychological Acceptability
MDS2	PAUT Person authentication, EMRG Emergency access
Standards	IEC 80001-1

CRI-AC-3 Credentials in service files

THE HOSPITAL · RANK 3

THREAT

Passwords, keys and interface credentials sit in plain text in device configuration backups, export files, service reports and installation notes. Whoever gets a copy, from a shared drive, an old laptop or a disposed device, gets the keys to the clinical systems they describe.

MITIGATION PROMPTS (ON THE CARD)

1. Where do configuration backups and service reports keep credentials?
2. Who can read exported device files on shared drives?
3. Are secrets removed before files leave the device?

MITIGATION PRINCIPLE

Secrets never appear in configuration exports, logs or documents that leave the device.

DESIGN MEASURES

1. Store device and interface secrets in a protected store and redact them from exports and service reports.
2. Scan shared drives and ticket systems for clinical system credentials and rotate any found.
3. Wipe credentials when devices are decommissioned, returned or sent for repair.

MAPPINGS

STRIDE	I Information disclosure, E Elevation of privilege
CAPEC	CAPEC-406 Dumpster Diving
CWE	CWE-256 Plaintext Storage of a Password CWE-522 Insufficiently Protected Credentials
ATT&CK	T1552.001 Credentials In Files
EMB3D	TID-329 Improper Password Storage TID-226 Device leaks security information in logs
MDS2	STCF Data storage confidentiality, SAHD System and application hardening
Standards	IEC 81001-5-1

CRI-AC-2 Badges cloned, shared and left in

THE HOSPITAL · RANK 2

THREAT

Proximity badges and smartcards give access to doors, drug rooms and clinical systems. Cards that are easy to clone, left in readers or lent to colleagues let someone else walk into restricted areas or act as the card holder on clinical systems.

MITIGATION PROMPTS (ON THE CARD)

1. How easily can your badges be cloned?
2. Where is a second factor needed beyond the badge?
3. What happens when a badge is left in a reader?

MITIGATION PRINCIPLE

A badge proves who is present only when it is hard to copy and backed by a second factor where it matters.

DESIGN MEASURES

1. Use badges with cryptographic authentication rather than readable serial numbers.
2. Require a PIN or biometric with the badge for controlled drugs, prescribing and restricted areas.
3. Remove the session automatically when the card leaves the reader.

MAPPINGS

STRIDE	S Spoofing
LINDDUN	I Identifying
CAPEC	CAPEC-390 Bypassing Physical Security
CWE	CWE-654 Reliance on a Single Factor in a Security Decision CWE-308 Use of Single-factor Authentication
MDS2	PAUT Person authentication, PLOK Physical locks
Standards	ISO 27799

CRI-CD · THE HOSPITAL · 13 ENTRIES

Continuity and Downtime

Estate-wide ransomware, shared services, backups, restore validation, downtime procedures and copies, diversion, incident communications and extortion.

https://ostering.com/taxonomies/hospitals-and-medical-devices/continuity-and-downtime/

CRI-CD-A Ransomware takes the whole estate

† CARE DELAYED OR WRONG THE HOSPITAL · RANK A

THREAT

Clinical and corporate systems share networks, accounts and management tools, so ransomware reaches records, imaging, labs, pharmacy and device servers at once. The hospital loses sight of its patients, diverts ambulances and cancels care for weeks while everything is rebuilt.

MITIGATION PROMPTS (ON THE CARD)

1. Which clinical services would keep running if the corporate estate fell?
2. What do clinical and corporate systems share: accounts, tools, networks?
3. How long would rebuilding the core clinical services take?

SEEN IN PUBLIC

WannaCry and the NHS, 2017. WannaCry ransomware disrupted at least 81 of England's 236 NHS trusts and infected 595 GP practices; the NAO estimated over 19,000 appointments were cancelled, and some trusts diverted ambulances. Sources: NAO: Investigation, WannaCry cyber attack and the NHS; GOV.UK: Foreign Office Minister condemns North Korean actor for WannaCry attacks

Conti attack on Ireland's HSE, 2021. Conti ransomware encrypted about 80% of the Health Service Executive's IT environment and about 700 GB of data was taken; the HSE shut its national IT down and took around four months to recover fully. PwC's independent post-incident review was published in December 2021. Sources: HSE: Conti cyber attack on the HSE, full report (PwC); HHS HC3: Lessons learned from the HSE cyber attack

Ascension, 2024. A ransomware attack took Ascension's electronic health records offline across its hospitals, staff worked on paper and some ambulances were diverted; data on about 5.6 million people was taken. Sources: BleepingComputer: Ascension health data of 5.6 million stolen in ransomware attack

MITIGATION PRINCIPLE

Design so that losing the corporate estate leaves a core of clinical care running.

DESIGN MEASURES

1. Segment clinical systems and devices so that a compromise of office IT cannot encrypt them.
2. Define the minimum clinical service that must survive and engineer its systems to run in isolation.
3. Rehearse an estate-wide outage with clinicians, not only IT, at least yearly.

MAPPINGS

STRIDE	D Denial of service, T Tampering
CAPEC	CAPEC-441 Malicious Logic Insertion
CWE	CWE-1220 Insufficient Granularity of Access Control
ATT&CK	T1486 Data Encrypted for Impact T1489 Service Stop T1490 Inhibit System Recovery
MDS2	MLDP Malware detection and protection, DTBK Data backup and disaster recovery
Standards	IEC 80001-1 ISO 27799

CRI-CD-K A shared service stops many hospitals

† CARE DELAYED OR WRONG THE HOSPITAL · RANK K

THREAT

Pathology, imaging, radiotherapy planning or IT is provided by one company or one hub for many hospitals. When it is attacked, every hospital it serves loses that service together, with no local fallback, and operations, transfusions and cancer treatment stop across a region.

MITIGATION PROMPTS (ON THE CARD)

1. Which clinical services come from one supplier shared by many hospitals?
2. What local fallback exists if that supplier is attacked?
3. Who coordinates across the region when a shared service fails?

SEEN IN PUBLIC

Synnovis pathology attack, London, 2024. Ransomware at Synnovis, pathology provider to King's College Hospital and Guy's and St Thomas', led to thousands of postponed operations and appointments and an appeal for O-type blood donors. In June 2025 King's confirmed a patient had died unexpectedly during the attack, with a long wait for a blood test result among the contributing factors; the local care board reported 170 patients harmed, mostly low harm. Sources: The Register: Qilin ransomware attack on NHS supplier contributed to patient fatality; Digital Health: Patient death linked to cyber attack on NHS pathology provider

Elekta cloud outage, 2021. Ransomware hit Elekta's first-generation US cloud service for radiation oncology software, and about 170 US health systems were affected; some cancer centres could not treat patients for over a week because treatment programming was held in the cloud. Sources: Compliancy Group: Healthcare vendor ransomware attack, 170 health systems hit; Yale Daily News: YNHHS pauses radiotherapy treatment for six days

MITIGATION PRINCIPLE

No single supplier or hub should be able to stop a clinical service across a region without a tested fallback.

DESIGN MEASURES

1. Map which clinical services depend on a shared provider and what each hospital does without it.
2. Contract for and test fallback capacity, such as mutual aid between laboratories or a second planning system.
3. Require shared providers to show segregation between customers so one attack does not stop all of them.

MAPPINGS

STRIDE	D Denial of service
CWE	CWE-1357 Reliance on Insufficiently Trustworthy Component
ATT&CK	T1199 Trusted Relationship T1486 Data Encrypted for Impact
MDS2	DTBK Data backup and disaster recovery
Standards	IEC 80001-1

CRI-CD-Q Backups reachable from what they protect

† CARE DELAYED OR WRONG THE HOSPITAL · RANK Q

THREAT

Backups of records, images and device configurations are online, writable and run by the same accounts as production. Attackers find and destroy them before encrypting, so restoring takes weeks of rebuilding rather than days of recovery.

MITIGATION PROMPTS (ON THE CARD)

1. Which backups would survive a full compromise of the estate?
2. Do backups use the same accounts as production?
3. How long would a restore from the offline copy take?

MITIGATION PRINCIPLE

At least one copy of every clinical system's data and configuration survives a full compromise of the estate.

DESIGN MEASURES

1. Keep immutable or offline copies managed by separate credentials that the main directory cannot reach.
2. Back up device configurations, drug libraries and interface definitions, not only databases.
3. Test full restores of clinical systems on a schedule and time them.

MAPPINGS

STRIDE	D Denial of service, T Tampering
CAPEC	CAPEC-607 Obstruction
CWE	CWE-732 Incorrect Permission Assignment for Critical Resource
ATT&CK	T1490 Inhibit System Recovery T1485 Data Destruction
MDS2	DTBK Data backup and disaster recovery
Standards	IEC 80001-1 ISO 27799

CRI-CD-J Restored data nobody has checked

† CARE DELAYED OR WRONG THE HOSPITAL · RANK J

THREAT

After an outage, systems are restored from backups and paper records are typed back in, but nobody checks that results, orders, allergies and medication histories are complete and unaltered. Missing or tampered clinical data flows back into care looking trustworthy.

MITIGATION PROMPTS (ON THE CARD)

1. How do you check that restored clinical data is complete?
2. Who verifies records typed back in from paper?
3. Could tampered data return with the restore unnoticed?

MITIGATION PRINCIPLE

Recovered clinical data is verified as complete and unaltered before clinicians rely on it.

DESIGN MEASURES

1. Hash and sign clinical data at backup so restored records can be checked for tampering.
2. Reconcile results, orders and medication given during downtime against the restored record, with clinical sign-off.
3. Flag records touched during the outage window so clinicians know to double-check them.

MAPPINGS

STRIDE	T Tampering, R Repudiation
CAPEC	CAPEC-184 Software Integrity Attack
CWE	CWE-354 Improper Validation of Integrity Check Value CWE-353 Missing Support for Integrity Check
ATT&CK	T1565.001 Stored Data Manipulation
MDS2	IGAU Health data integrity and authenticity, DTBK Data backup and disaster recovery
Standards	IEC 80001-1

CRI-CD-10 Downtime procedures nobody has practised

† CARE DELAYED OR WRONG THE HOSPITAL · RANK 10

THREAT

Paper forms, manual ordering, handwritten labels and runners exist on paper but have never been tried at scale. When systems go down for weeks, staff improvise, errors multiply in prescribing, identification and results, and staff exhaust themselves keeping it running.

MITIGATION PROMPTS (ON THE CARD)

1. When were downtime procedures last practised at scale?
2. Who staffs runners, manual ordering and paper reconciliation?
3. How long could manual working last before errors climb?

SEEN IN PUBLIC

Synnovis pathology attack, London, 2024. Ransomware at Synnovis, pathology provider to King's College Hospital and Guy's and St Thomas', led to thousands of postponed operations and appointments and an appeal for O-type blood donors. In June 2025 King's confirmed a patient had died unexpectedly during the attack, with a long wait for a blood test result among the contributing factors; the local care board reported 170 patients harmed, mostly low harm. Sources: The Register: Qilin ransomware attack on NHS supplier contributed to patient fatality; Digital Health: Patient death linked to cyber attack on NHS pathology provider

Ascension, 2024. A ransomware attack took Ascension's electronic health records offline across its hospitals, staff worked on paper and some ambulances were diverted; data on about 5.6 million people was taken. Sources: BleepingComputer: Ascension health data of 5.6 million stolen in ransomware attack

MITIGATION PRINCIPLE

Manual working is a planned, practised and staffed mode of the hospital, not an improvisation.

DESIGN MEASURES

1. Keep downtime packs on every ward with forms, label stock and contact lists, checked monthly.
2. Run downtime drills that include pharmacy, labs, imaging and portering, and record what failed.
3. Plan rotas and extra staff for long outages so manual working is sustainable for weeks.

MAPPINGS

STRIDE	D Denial of service
ATT&CK	T0826 Loss of Availability
MDS2	DTBK Data backup and disaster recovery
Standards	IEC 80001-1

CRI-CD-9 Devices that stop without their server

† DIRECT HARM THE HOSPITAL · RANK 9

THREAT

Devices need a licence server, drug library server, worklist or vendor cloud to start or keep working. When the back end is encrypted or cut off, pumps, modalities and analysers refuse to run or lock into unsafe defaults, though they could work alone.

MITIGATION PROMPTS (ON THE CARD)

1. Which devices refuse to start without their server or licence?
2. What defaults do devices fall back to when the back end is gone?
3. Could these devices treat or diagnose safely on their own?

MITIGATION PRINCIPLE

A device that can treat or diagnose safely on its own keeps doing so when its back end is gone.

DESIGN MEASURES

1. Require devices to keep working in a safe local mode, with their last good configuration, when servers are lost.
2. Ask suppliers about back-end dependencies and grace periods in procurement and test them before go-live.
3. Document how to run each critical device without its network, and practise it.

MAPPINGS

STRIDE	D Denial of service
CWE	CWE-754 Improper Check for Unusual or Exceptional Conditions CWE-1357 Reliance on Insufficiently Trustworthy Component
ATT&CK	T0826 Loss of Availability T0816 Device Restart/Shutdown
MDS2	DTBK Data backup and disaster recovery, CONN Connectivity capabilities
Standards	IEC 80001-1 IEC TR 60601-4-5 FDA premarket

CRI-CD-8 Diversion overloads the neighbours

† CARE DELAYED OR WRONG THE HOSPITAL · RANK 8

THREAT

A hospital that loses its systems diverts ambulances and transfers to nearby hospitals, which are already busy. Travel times rise for critically ill patients and the neighbours run short of beds and staff, so one attack degrades emergency care across a region.

MITIGATION PROMPTS (ON THE CARD)

1. Which neighbouring hospitals absorb your patients if you divert?
2. Do regional plans assume a hospital lost to a cyberattack?
3. How is the extra load shared before it lands?

SEEN IN PUBLIC

University Hospital Düsseldorf, 2020. Ransomware took down systems at University Hospital Düsseldorf and it stopped taking emergency admissions; a woman sent to a hospital in another city died. Prosecutors opened a homicide inquiry but closed it, concluding her condition alone caused her death and the delay did not affect the outcome. Sources: MIT Technology Review: A patient has died after ransomware hackers hit a German hospital; Born's Tech and Windows World: ransomware at Uniklinik Düsseldorf not responsible for death

MITIGATION PRINCIPLE

Regional plans assume a hospital can be lost to a cyberattack and share the load before it lands.

DESIGN MEASURES

1. Agree cyber diversion triggers and capacity with neighbouring hospitals and ambulance services in advance.
2. Keep a way to update diversion status that does not depend on the affected hospital's systems.
3. Plan which time-critical services, such as stroke and cardiac care, must stay open and how.

MAPPINGS

STRIDE	D Denial of service
ATT&CK	T0826 Loss of Availability
Standards	IEC 80001-1

CRI-CD-7 One update takes the estate down

† CARE DELAYED OR WRONG THE HOSPITAL · RANK 7

THREAT

A trusted security agent, operating system or management tool pushes a faulty or malicious update to every machine at once. Clinical workstations, servers and device consoles fail together, and the hospital cannot recover them faster than it can visit each one.

MITIGATION PROMPTS (ON THE CARD)

1. Which tools can push an update to every machine at once?
2. Are updates staged so critical systems can be held back?
3. How quickly could you stop and roll back a bad update?

SEEN IN PUBLIC

CrowdStrike update outage, 2024. A faulty CrowdStrike security update crashed Windows computers worldwide; hospitals lost systems for hours and some, such as Mass General Brigham, cancelled non-urgent surgeries and visits. Sources: STAT: Hospitals cancel appointments in global tech outage; WBUR: Mass General Brigham cancels non-urgent surgeries

MITIGATION PRINCIPLE

Updates reach critical clinical systems in stages, with a way to stop and roll back before all are affected.

DESIGN MEASURES

1. Stage updates to clinical systems in rings, holding critical areas back until earlier rings are healthy.
2. Keep a tested way to recover machines in bulk without the failed tool, such as rebuild images on local media.
3. Hold a minimum set of devices on a different platform or update channel for continuity.

MAPPINGS

STRIDE	D Denial of service, T Tampering
CAPEC	CAPEC-186 Malicious Software Update
CWE	CWE-494 Download of Code Without Integrity Check
ATT&CK	T1195.002 Compromise Software Supply Chain
EMB3D	TID-217 Remotely Initiated Updates Can Cause DoS
MDS2	CSUP Cybersecurity product upgrades, DTBK Data backup and disaster recovery
Standards	IEC 80001-1

CRI-CD-6 Downtime copies that go down too

† CARE DELAYED OR WRONG THE HOSPITAL · RANK 6

THREAT

Read-only downtime viewers, medication lists and printed reports depend on the same network, directory or storage as the main record. When the outage comes they are encrypted or stale, and clinicians lose allergies, drug charts and care plans exactly when they need them.

MITIGATION PROMPTS (ON THE CARD)

1. What do downtime viewers and printed reports depend on?
2. Would downtime copies survive the same outage as the record?
3. How current are the downtime copies at any moment?

MITIGATION PRINCIPLE

Downtime copies are independent of the systems whose failure they cover.

DESIGN MEASURES

1. Keep downtime copies on standalone devices per ward, refreshed often and not joined to the main directory.
2. Print or cache critical summaries such as medication charts and allergies on a schedule.
3. Test that downtime copies open with the network, directory and main storage all unavailable.

MAPPINGS

STRIDE	D Denial of service
LINDDUN	DD Data disclosure
CWE	CWE-1357 Reliance on Insufficiently Trustworthy Component
ATT&CK	T1486 Data Encrypted for Impact
MDS2	DTBK Data backup and disaster recovery, STCF Data storage confidentiality
Standards	IEC 80001-1

CRI-CD-5 Incident communications on compromised systems

† CARE DELAYED OR WRONG THE HOSPITAL · RANK 5

THREAT

The incident plan relies on email, VoIP phones, paging and the intranet to call staff in and coordinate. Those same systems are down or untrusted, so command cannot reach staff, the ambulance service or the public, and attackers may read the response.

MITIGATION PROMPTS (ON THE CARD)

1. How would incident command reach staff with email and phones down?
2. Which communication channels share fate with the systems under attack?
3. Could attackers be reading the response?

MITIGATION PRINCIPLE

The hospital can command its response with systems that do not share the fate of the ones under attack.

DESIGN MEASURES

1. Provide out-of-band communications for incident command, such as separate phones, radios or a hosted service.
2. Keep printed contact lists and call-in cascades that work without the directory.
3. Assume email and chat are being read during an incident and move sensitive decisions off them.

MAPPINGS

STRIDE	D Denial of service, I Information disclosure
ATT&CK	T1489 Service Stop
Standards	IEC 80001-1

CRI-CD-4 No planned restore order

THE HOSPITAL · RANK 4

THREAT

Nobody has worked out which systems must come back first and what they depend on. Teams restore systems that cannot run without the directory, DNS, integration engine or certificates, and clinical priorities wait behind whatever IT reaches first.

MITIGATION PROMPTS (ON THE CARD)

1. Which systems must be restored first for clinical care?
2. What technical dependencies does each priority system have?
3. When was the restore order last tested?

MITIGATION PRINCIPLE

The restore order follows clinical priority and real technical dependencies, both written down and tested.

DESIGN MEASURES

1. Map dependencies of each clinical system, including identity, DNS, time, integration and licences.
2. Agree a restore order with clinical leads and keep it with the backups, offline.
3. Rehearse restoring the top tier of clinical services from bare infrastructure.

MAPPINGS

STRIDE	D Denial of service
ATT&CK	T1490 Inhibit System Recovery
MDS2	DTBK Data backup and disaster recovery
Standards	IEC 80001-1

CRI-CD-3 Extortion deadlines rush the recovery

† CARE DELAYED OR WRONG THE HOSPITAL · RANK 3

THREAT

Attackers set publication deadlines and contact staff, patients and the press while the hospital is still restoring. Under that pressure leaders skip validation, restore from unchecked backups or reconnect early, and the attackers' access or damaged data comes back with the services.

MITIGATION PROMPTS (ON THE CARD)

1. Who decides on reconnection, and on what evidence?
2. How will publication threats be handled without driving technical choices?
3. Will you rebuild from known-good images even if it is slower?

SEEN IN PUBLIC

Conti attack on Ireland's HSE, 2021. Conti ransomware encrypted about 80% of the Health Service Executive's IT environment and about 700 GB of data was taken; the HSE shut its national IT down and took around four months to recover fully. PwC's independent post-incident review was published in December 2021. Sources: HSE: Conti cyber attack on the HSE, full report (PwC); HHS HC3: Lessons learned from the HSE cyber attack

MITIGATION PRINCIPLE

Recovery steps are decided on clinical and technical evidence, not on the extortion clock.

DESIGN MEASURES

1. Agree in advance who decides on reconnection and what evidence they need, independent of any ransom deadline.
2. Prepare holding statements and patient lines so publication threats do not drive technical decisions.
3. Rebuild from known-good images even when that is slower than restoring in place.

MAPPINGS

STRIDE	T Tampering, D Denial of service
ATT&CK	T1657 Financial Theft T1486 Data Encrypted for Impact
MDS2	DTBK Data backup and disaster recovery
Standards	IEC 80001-1

CRI-CD-2 Payments and claims stop flowing

THE HOSPITAL · RANK 2

THREAT

Claims, eligibility checks and pharmacy payments run through a single clearing service or payer platform. When it is attacked, providers cannot verify cover or get paid, pharmacies cannot dispense on account, and smaller practices run out of cash within weeks.

MITIGATION PROMPTS (ON THE CARD)

1. Which payment or eligibility service would stop dispensing or billing?
2. How long could smaller providers survive without payments?
3. Can care continue when cover cannot be checked?

SEEN IN PUBLIC

Change Healthcare, 2024. Ransomware at Change Healthcare, which handles about one in three US health transactions, left many providers and pharmacies unable to process claims and prescriptions for weeks; the data of about 192.7 million people was taken. Sources: Becker's: Change Healthcare data breach toll reaches 192.7 million; Fierce Healthcare: UnitedHealth estimates 190M people impacted

MITIGATION PRINCIPLE

Clinical care continues when payment and eligibility services do not, and providers can survive a long payment outage.

DESIGN MEASURES

1. Agree with payers how care is authorised and paid when eligibility services are down.
2. Keep a second route to submit claims and check cover, tested at least yearly.
3. Plan financial reserves or emergency funding for a payment outage of several weeks.

MAPPINGS

STRIDE	D Denial of service
CWE	CWE-1357 Reliance on Insufficiently Trustworthy Component
ATT&CK	T1486 Data Encrypted for Impact

CRI-TR · BOTH DECKS · 10 ENTRIES

Structural hazards

Ten structural hazards of hospitals and medical devices as a whole. Both decks carry them, ranked 1 (highest) to 10.

https://ostering.com/taxonomies/hospitals-and-medical-devices/structural-hazards/

CRI-TR-1 Life before login

† CARE DELAYED OR WRONG TRUMP 1 OF 10

THREAT

Clinical urgency beats every control that slows care. Staff will bypass, share or switch off any security that delays treatment, so a design that only works when people comply fails on the busiest night, and a control that fails closed can harm a patient.

MITIGATION PROMPTS (ON THE CARD)

1. Which security steps slow care in an emergency, and by how long?
2. Is the secure path also the fastest one on the busiest night?
3. Which controls fail closed where failing closed could harm a patient?

MITIGATION PRINCIPLE

Design security so the safe and secure path is also the fastest path in an emergency.

DESIGN MEASURES

1. Time every security step in real clinical workflows and set targets in seconds.
2. Provide accountable emergency access instead of hoping staff will not need it.
3. Decide, per function, whether failure should be open or closed, and justify it in the safety case.

MAPPINGS

STRIDE	E Elevation of privilege
CAPEC	CAPEC-416 Manipulate Human Behavior
CWE	CWE-655 Insufficient Psychological Acceptability
MDS2	EMRG Emergency access
Standards	IEC 80001-1 ISO 14971

CRI-TR-2 The device outlives its software

† CARE DELAYED OR WRONG TRUMP 2 OF 10

THREAT

Medical devices stay in service for ten to twenty years, while their operating systems and components lose support in a few. Hospitals run certified builds that cannot change, so known weaknesses stay open for most of a device's life.

MITIGATION PROMPTS (ON THE CARD)

1. How long will this device stay in service, and its software supported?
2. What happens to it once its operating system loses support?
3. Who plans the device's software life at purchase?

SEEN IN PUBLIC

Argus II retinal implant, 2020. Second Sight phased out its Argus II retinal implant and, after laying off most staff in March 2020, could no longer support its more than 350 recipients; patients were left with implants that could not be repaired and, in one case, could not get an MRI without the maker's input. Sources: IEEE Spectrum: Their bionic eyes are now obsolete and unsupported

MITIGATION PRINCIPLE

Plan the whole service life of a device's software at design and at purchase.

DESIGN MEASURES

1. Require a support roadmap for every third-party component and an end-of-support date in the contract.
2. Design devices so components can be updated without replacing the clinical function.
3. Budget and plan replacement or isolation before support ends, not after.

MAPPINGS

CWE	CWE-1104 Use of Unmaintained Third Party Components CWE-1329 Reliance on Component That is Not Updateable
MDS2	RDMP Roadmap for third-party components, SBOM Software bill of materials, CSUP Cybersecurity product upgrades
Standards	AAMI SW96 FDA premarket IEC 81001-5-1

CRI-TR-3 Nobody owns the bedside

† CARE DELAYED OR WRONG TRUMP 3 OF 10

THREAT

Clinical engineering, IT, the supplier and the ward each assume another owns a connected device's security. Patching, monitoring, configuration and incident response fall between them, and attackers find the gaps first.

MITIGATION PROMPTS (ON THE CARD)

1. Who owns the security of each connected device in this design?
2. Where do clinical engineering, IT, vendor and ward responsibilities meet?
3. Who responds first when a bedside device is compromised?

MITIGATION PRINCIPLE

Every connected device has a named owner for its security, across its whole life.

DESIGN MEASURES

1. Assign responsibilities for each device class in a written agreement between clinical engineering, IT and the supplier.
2. Keep one inventory of connected devices, shared by all owners, with a named contact per device.
3. Include connected devices in incident response playbooks with clear decision rights.

MAPPINGS

CWE	CWE-671 Lack of Administrator Control over Security
MDS2	SGUD Security guidance
Standards	IEC 80001-1

CRI-TR-4 Safety cases assume accidents

† CARE DELAYED OR WRONG TRUMP 4 OF 10

THREAT

Risk files and safety cases model random failures and honest mistakes. An adversary chooses the worst moment, defeats several safeguards together and hides the evidence, so controls judged independent fail at once and residual risk is far higher than the file says.

MITIGATION PROMPTS (ON THE CARD)

1. Does the safety risk file treat an adversary as a cause of hazards?
2. Which safeguards could one attacker defeat together?
3. How would the residual risk change if failures were deliberate?

MITIGATION PRINCIPLE

Treat intentional misuse as a cause of hazards in the safety risk file, not a separate concern.

DESIGN MEASURES

1. Link security threats to hazards in the ISO 14971 risk file and score them together.
2. Check that safeguards relied on as independent cannot be defeated by one compromise.
3. Reassess the safety case whenever a new vulnerability or attack technique affects the device.

MAPPINGS

CWE	CWE-1357 Reliance on Insufficiently Trustworthy Component
ATT&CK	T0880 Loss of Safety T0837 Loss of Protection
MDS2	IGAU Health data integrity and authenticity
Standards	ISO 14971 AAMI SW96 IEC TR 60601-4-5

CRI-TR-5 Alarm fatigue hides the attack

† CARE DELAYED OR WRONG TRUMP 5 OF 10

THREAT

Wards hear hundreds of alarms a shift, most of them false, so staff silence, widen or ignore them. Manipulated readings, suppressed alarms or a device behaving oddly blend into the noise and are noticed late, if at all.

MITIGATION PROMPTS (ON THE CARD)

1. How many alarms does each ward hear in a shift?
2. Would a manipulated alarm stand out from the noise?
3. Who can change alarm settings, and is that protected?

MITIGATION PRINCIPLE

Alarms are few, meaningful and protected from change, so an abnormal one gets attention.

DESIGN MEASURES

1. Reduce non-actionable alarms through tuning and clinical review before adding new ones.
2. Protect alarm limits and routing from unauthorised change and log every change.
3. Report alarm silencing and limit changes per device so unusual patterns are seen.

MAPPINGS

STRIDE	T Tampering, R Repudiation
CWE	CWE-778 Insufficient Logging
ATT&CK	T0832 Manipulation of View
MDS2	AUDT Audit controls, IGAU Health data integrity and authenticity
Standards	IEC 80001-1

CRI-TR-6 One supplier, many hospitals

† CARE DELAYED OR WRONG TRUMP 6 OF 10

THREAT

A handful of suppliers provide the record systems, laboratories, imaging platforms, remote service tools and clouds for most hospitals in a region or country. One compromise or one failure at a supplier becomes an incident at every customer together.

MITIGATION PROMPTS (ON THE CARD)

1. Which suppliers in this design also serve most nearby hospitals?
2. What would one supplier's compromise do to every customer at once?
3. How would you keep working without that supplier?

SEEN IN PUBLIC

Synnovis pathology attack, London, 2024. Ransomware at Synnovis, pathology provider to King's College Hospital and Guy's and St Thomas', led to thousands of postponed operations and appointments and an appeal for O-type blood donors. In June 2025 King's confirmed a patient had died unexpectedly during the attack, with a long wait for a blood test result among the contributing factors; the local care board reported 170 patients harmed, mostly low harm. Sources: The Register: Qilin ransomware attack on NHS supplier contributed to patient fatality; Digital Health: Patient death linked to cyber attack on NHS pathology provider

Change Healthcare, 2024. Ransomware at Change Healthcare, which handles about one in three US health transactions, left many providers and pharmacies unable to process claims and prescriptions for weeks; the data of about 192.7 million people was taken. Sources: Becker's: Change Healthcare data breach toll reaches 192.7 million; Fierce Healthcare: UnitedHealth estimates 190M people impacted

MITIGATION PRINCIPLE

Know where many hospitals share one supplier and keep a way to work without it.

DESIGN MEASURES

1. Map shared suppliers across the region and treat concentration as a risk to manage.
2. Require suppliers to separate customers so one breach does not reach all of them.
3. Plan mutual aid and fallbacks that do not use the same supplier.

MAPPINGS

STRIDE	D Denial of service
CWE	CWE-1357 Reliance on Insufficiently Trustworthy Component
ATT&CK	T1199 Trusted Relationship T1195.002 Compromise Software Supply Chain
MDS2	RMOT Remote service
Standards	IEC 80001-1

CRI-TR-7 Patch means revalidate

† CARE DELAYED OR WRONG TRUMP 7 OF 10

THREAT

Changing a certified device's software means verification by the maker and sometimes the regulator, and hospitals are told not to patch themselves. Fixes arrive months or years after the weakness is public, and the hospital must defend a device it is not allowed to change.

MITIGATION PROMPTS (ON THE CARD)

1. How long does a validated fix take to reach this device?
2. What may the hospital do while a fix is awaited?
3. Does the contract commit the maker to timely validated updates?

MITIGATION PRINCIPLE

Design and contract for timely, validated updates as part of the device, not an exception.

DESIGN MEASURES

1. Design devices so security updates can be verified quickly without re-certifying clinical function.
2. Agree update timelines and compensating controls in the purchase contract.
3. Isolate and monitor devices awaiting validated updates, with the supplier's guidance.

MAPPINGS

CWE	CWE-1329 Reliance on Component That is Not Updateable
EMB3D	TID-213 Faulty FW/SW Update Integrity Verification
MDS2	CSUP Cybersecurity product upgrades, RDMP Roadmap for third-party components
Standards	FDA premarket AAMI SW96 IEC 81001-5-1

CRI-TR-8 Every patient is a target

TRUMP 8 OF 10

THREAT

Health records are permanent, deeply personal and valuable for fraud, extortion, discrimination and intelligence. Every patient is a data subject whose information can be sold, published or used against them, long after the care has ended.

MITIGATION PROMPTS (ON THE CARD)

1. What patient data does this design collect that care doesn't need?
2. Which data would do most harm if sold or published?
3. How long is patient data kept after care ends?

SEEN IN PUBLIC

Vastaamo psychotherapy records, Finland, 2020. Therapy records of about 36,000 patients of the Vastaamo psychotherapy centre were stolen in 2018 and 2019; in October 2020, after the company refused to pay, patients were extorted individually. A Finnish court convicted the attacker in April 2024 and the appeal court upheld the conviction in 2025. Sources: Wikipedia: Vastaamo data breach; AP via NY1: Finnish hacker gets prison for accessing psychotherapy records

MITIGATION PRINCIPLE

Collect, keep and expose only what care needs, and protect the most sensitive data most strongly.

DESIGN MEASURES

1. Classify record categories by sensitivity and apply stronger controls to the most sensitive.
2. Minimise copies of patient data in secondary systems, exports and test environments.
3. Give patients a way to see who has accessed their record.

MAPPINGS

STRIDE	I Information disclosure
LINDDUN	L Linking, I Identifying, DD Data disclosure, U Unawareness and unintervenability, Nc Non-compliance
CWE	CWE-359 Exposure of Private Personal Information to an Unauthorized Actor
MDS2	MPII Management of private data, STCF Data storage confidentiality, DIDT Health data de-identification
Standards	ISO 27799

CRI-TR-9 The hospital never closes

† CARE DELAYED OR WRONG TRUMP 9 OF 10

THREAT

Hospitals run every hour of every day with no maintenance window. Patching, testing and recovery all compete with care, and the only way to switch a hospital off safely is to divert patients elsewhere.

MITIGATION PROMPTS (ON THE CARD)

1. When can this system be patched, tested or restored without stopping care?
2. What does the design assume about maintenance windows?
3. Is diversion the only way to take this service offline safely?

MITIGATION PRINCIPLE

Build maintenance and recovery into the design so they do not require stopping care.

DESIGN MEASURES

1. Design redundant clinical systems so one side can be updated while the other runs.
2. Plan maintenance with clinical leads around activity, not around IT convenience.
3. Treat the ability to recover without closing as a design requirement.

MAPPINGS

STRIDE	D Denial of service
ATT&CK	T0826 Loss of Availability
MDS2	DTBK Data backup and disaster recovery, CSUP Cybersecurity product upgrades
Standards	IEC 80001-1

CRI-TR-10 Hospitals are strategic targets

† CARE DELAYED OR WRONG TRUMP 10 OF 10

THREAT

Hospitals are critical infrastructure. Criminals target them because they pay, and states may pre-position in them or disrupt them in a crisis or conflict to cause fear and overwhelm emergency response. Plans built for accidents and petty crime do not survive a determined adversary.

MITIGATION PROMPTS (ON THE CARD)

1. Does the design assume a patient, capable adversary or just criminals?
2. What would a state actor gain by disrupting this system in a crisis?
3. Which plans would fail against a deliberate, coordinated attack?

MITIGATION PRINCIPLE

Plan for a patient, capable adversary who wants disruption, not only for criminals who want money.

DESIGN MEASURES

1. Include state-level scenarios, such as simultaneous attacks on several hospitals, in continuity planning.
2. Share threat intelligence with sector bodies and national authorities and act on it.
3. Hunt for long-term access in clinical and device networks, not only for ransomware.

MAPPINGS

STRIDE	D Denial of service, E Elevation of privilege
ATT&CK	T1078 Valid Accounts T1133 External Remote Services
Standards	IEC 62443 IEC 80001-1

Public cases and sources

Each case was checked against public sources. Entries cite a case where it shows the threat in practice; attribution is given only as officially stated.

Case	What happened	Entries	Sources
WannaCry and the NHS, 2017 12 May 2017	WannaCry ransomware disrupted at least 81 of England's 236 NHS trusts and infected 595 GP practices; the NAO estimated over 19,000 appointments were cancelled, and some trusts diverted ambulances. Attribution: attributed by the UK and US governments to North Korea (December 2017)	CRI-IR-9, CRI-NW-A, CRI-NW-K, CRI-SV-J, CRI-AC-Q, CRI-CD-A	NAO: Investigation, WannaCry cyber attack and the NHS GOV.UK: Foreign Office Minister condemns North Korean actor for WannaCry attacks
University Hospital Düsseldorf, 2020 September 2020	Ransomware took down systems at University Hospital Düsseldorf and it stopped taking emergency admissions; a woman sent to a hospital in another city died. Prosecutors opened a homicide inquiry but closed it, concluding her condition alone caused her death and the delay did not affect the outcome. Attribution: unattributed (DoppelPaymer ransomware reported; no official attribution)	CRI-EC-K, CRI-CD-8	MIT Technology Review: A patient has died after ransomware hackers hit a German hospital Born's Tech and Windows World: ransomware at Uniklinik Düsseldorf not responsible for death
Conti attack on Ireland's HSE, 2021 14 May 2021	Conti ransomware encrypted about 80% of the Health Service Executive's IT environment and about 700 GB of data was taken; the HSE shut its national IT down and took around four months to recover fully. PwC's independent post-incident review was published in December 2021. Attribution: Conti ransomware group (criminal); no state attribution	CRI-AC-Q, CRI-CD-A, CRI-CD-3	HSE: Conti cyber attack on the HSE, full report (PwC) HHS HC3: Lessons learned from the HSE cyber attack
Synnovis pathology attack, London, 2024 3 June 2024	Ransomware at Synnovis, pathology provider to King's College Hospital and Guy's and St Thomas', led to thousands of postponed operations and appointments and an appeal for O-type blood donors. In June 2025 King's confirmed a patient had died unexpectedly during the attack, with a long wait for a blood test result among the contributing factors; the local care board reported 170 patients harmed, mostly low harm. Attribution: Qilin ransomware group (criminal)	CRI-LD-Q, CRI-CD-K, CRI-CD-10, CRI-TR-6	The Register: Qilin ransomware attack on NHS supplier contributed to patient fatality Digital Health: Patient death linked to cyber attack on NHS pathology provider
Change Healthcare, 2024 February 2024	Ransomware at Change Healthcare, which handles about one in three US health transactions, left many providers and pharmacies unable to process claims and prescriptions for weeks; the data of about 192.7 million people was taken. Attribution: ALPHV/BlackCat ransomware group (criminal)	CRI-RC-K, CRI-CD-2, CRI-TR-6	Becker's: Change Healthcare data breach toll reaches 192.7 million Fierce Healthcare: UnitedHealth estimates 190M people impacted
Ascension, 2024 8 May 2024	A ransomware attack took Ascension's electronic health records offline across its hospitals, staff worked on paper and some ambulances were diverted; data on about 5.6 million people was taken. Attribution: Black Basta ransomware reported by the media; not confirmed by Ascension	CRI-EC-K, CRI-CD-A, CRI-CD-10	BleepingComputer: Ascension health data of 5.6 million stolen in ransomware attack

Advanced and NHS 111, 2022 4 August 2022	Ransomware at software supplier Advanced disrupted the Adastra system used by NHS 111 and out-of-hours services, and exposed data on about 80,000 people. The UK Information Commissioner fined Advanced £3.07 million in March 2025. Attribution: LockBit ransomware group (criminal)	CRI-EC-A	ICO: Software provider fined £3m following 2022 ransomware attack
Vastaamo psychotherapy records, Finland, 2020 October 2020 (extortion); theft 2018 to 2019	Therapy records of about 36,000 patients of the Vastaamo psychotherapy centre were stolen in 2018 and 2019; in October 2020, after the company refused to pay, patients were extorted individually. A Finnish court convicted the attacker in April 2024 and the appeal court upheld the conviction in 2025. Attribution: convicted individual (Aleksanteri Kivimäki), criminal	CRI-RC-Q, CRI-TR-8	Wikipedia: Vastaamo data breach AP via NY1: Finnish hacker gets prison for accessing psychotherapy records
CrowdStrike update outage, 2024 19 July 2024	A faulty CrowdStrike security update crashed Windows computers worldwide; hospitals lost systems for hours and some, such as Mass General Brigham, cancelled non-urgent surgeries and visits. Attribution: not an attack (faulty vendor update)	CRI-CD-7	STAT: Hospitals cancel appointments in global tech outage WBUR: Mass General Brigham cancels non-urgent surgeries
Medtronic MiniMed insulin pumps, 2019 27 June 2019	The FDA warned that certain older Medtronic MiniMed insulin pumps could be reached over their radio link by someone nearby and their settings changed; Medtronic recalled them and offered replacements, as the pumps could not be updated. Attribution: not applicable (vulnerability, no reported attack)	CRI-BW-A	Infosecurity: Insulin pumps recalled by FDA for cybersecurity risks Becker's: Medtronic recalls insulin pumps that can be wirelessly hacked
Abbott (St. Jude Medical) pacemakers, 2017 29 August 2017	The FDA approved a firmware update for about 465,000 radio-enabled Abbott pacemakers in the US to stop unauthorised reprogramming; patients had to visit a clinic to have it applied, weighing a small risk of update failure. Attribution: not applicable (vulnerability, no reported attack)	CRI-IM-K	Help Net Security: Patients with St. Jude pacemakers called in for firmware update CSO: 465,000 Abbott pacemakers vulnerable to hacking need a firmware fix
Medtronic Conexus telemetry, 2019 21 March 2019	US government advisories warned that the Conexus radio protocol used by Medtronic implantable defibrillators, clinic programmers and home monitors had no authentication or encryption, so someone nearby could read or change device settings. Attribution: not applicable (vulnerability, no reported attack)	CRI-IM-A, CRI-IM-4	CISA: ICS Medical Advisory ICSMA-19-080-01
Hospira Symbiq infusion pumps, 2015 31 July 2015	The FDA advised hospitals to stop using Hospira Symbiq infusion pumps because they could be accessed remotely over the hospital network and their dosing changed. Attribution: not applicable (vulnerability, no reported attack)	CRI-MD-K	MDDI: FDA, stop using infusion pump vulnerable to hacking
Contec CMS8000 patient monitors, 2025 30 January 2025	CISA and the FDA warned that Contec CMS8000 patient monitors made hidden connections to a hard-coded internet address, could download and run unverified files, and sent patient data in plain text when a patient was connected; with no fix available, CISA advised unplugging them. A researcher later argued it was more likely insecure design than deliberate backdoor. Attribution: not applicable (vulnerability, no reported attack)	CRI-PM-8	CISA: Fact sheet, Contec CMS8000 contains a backdoor The Hacker News: CISA and FDA warn of critical backdoor in Contec CMS8000
PwnedPiper pneumatic tubes, 2021 2 August 2021	Armis disclosed nine vulnerabilities in Swisslog Translogic pneumatic tube system stations, used by thousands of hospitals to move samples and drugs, including unsigned firmware updates that could let an attacker take over stations. Attribution: not applicable (research disclosure)	CRI-FB-8	The Register: PwnedPiper flaws in Swisslog pneumatic tube systems Health-ISAC: Armis discovers 9 vulnerabilities in hospital infrastructure

SweynTooth Bluetooth flaws, 2020 3 March 2020	The FDA warned that SweynTooth flaws in Bluetooth Low Energy chips used in pacemakers, glucose monitors, insulin pumps and other devices could let someone nearby crash a device, stop it working or bypass security. Attribution: not applicable (research disclosure)	CRI-BW-8, CRI-BW-7, CRI-NW-7, CRI-SV-3	RAPS: FDA warns of cybersecurity vulnerabilities in pacemakers and other BLE devices HPN: FDA informs about potential vulnerabilities in medical devices with Bluetooth Low Energy
URGENT/11, 2019 1 October 2019	The FDA warned that 11 vulnerabilities in IPnet, a third-party network stack inside several embedded operating systems, could let attackers take over or crash medical devices and hospital network equipment, and that manufacturers might not know their products contained it. Attribution: not applicable (research disclosure)	CRI-PM-9, CRI-MD-7, CRI-NW-10, CRI-SV-3	Healthcare IT News: URGENT/11, FDA issues alert
MDhex, GE patient monitoring, 2020 23 January 2020	CISA published six vulnerabilities (MDhex) in GE Healthcare CARESCAPE telemetry servers, central stations and related patient monitoring products, including hard-coded credentials, that could let an attacker change alarm settings or make devices unusable. Attribution: not applicable (research disclosure)	CRI-PM-A, CRI-PM-9	Help Net Security: MDhex vulnerabilities open GE patient monitoring devices to attackers Computer Weekly: NHS alerted to severe vulnerabilities in GE health equipment
Elekta cloud outage, 2021 20 April 2021	Ransomware hit Elekta's first-generation US cloud service for radiation oncology software, and about 170 US health systems were affected; some cancer centres could not treat patients for over a week because treatment programming was held in the cloud. Attribution: unattributed	CRI-IR-K, CRI-SV-Q, CRI-CD-K	Compliancy Group: Healthcare vendor ransomware attack, 170 health systems hit Yale Daily News: YNHHS pauses radiotherapy treatment for six days
Open PACS servers, 2019 September 2019	Greenbone found about 590 imaging archive (PACS) servers reachable on the internet without protection, exposing records of about 24 million patients and hundreds of millions of images; an update later counted over a billion images. Attribution: not applicable (research finding)	CRI-IR-5, CRI-IN-J, CRI-NW-J	Help Net Security: Confidential data of 24.3 million patients discovered online HIPAA Journal: Exposed medical image total rises to 1.19 billion
Leaking Beeps, 2016 2016	Trend Micro research showed that pager messages sent by US hospitals were unencrypted and could be read with cheap radio equipment, exposing patient names, diagnoses and treatment details. Attribution: not applicable (research finding)	CRI-CC-10	Trend Micro: Leaking Beeps, unencrypted pager messages in the healthcare industry Trend Micro: Are pagers leaking your patients' PHI?
Argus II retinal implant, 2020 2019 to 2020	Second Sight phased out its Argus II retinal implant and, after laying off most staff in March 2020, could no longer support its more than 350 recipients; patients were left with implants that could not be repaired and, in one case, could not get an MRI without the maker's input. Attribution: not applicable (manufacturer withdrawal)	CRI-IM-8, CRI-SV-4, CRI-TR-2	IEEE Spectrum: Their bionic eyes are now obsolete and unsupported
DICOM files carrying malware, 2019 April 2019	Cylera researchers showed that the DICOM file format allows an image file to also be a working Windows executable, so malware could hide inside medical images protected as patient data (CVE-2019-11687). Attribution: not applicable (research disclosure)	CRI-IR-10, CRI-IN-J, CRI-EC-9	NVD: CVE-2019-11687 GovInfoSecurity: Researchers, malware can be hidden in medical images

NHS Dumfries and Galloway, 2024 15 March 2024	A ransomware group stole data from NHS Dumfries and Galloway, claiming 3 TB, and published clinical data on patients to pressure the health board; the board said records were not altered and care continued. Attribution: INC Ransom group (criminal)	CRI-RC-K	Help Net Security: NHS Scotland confirms ransomware attackers leaked patients' data Digital Health: NHS Dumfries and Galloway working with NCSC after 3TB data leak
Brno University Hospital, 2020 12 to 13 March 2020	A cyberattack forced Brno University Hospital, home to one of the Czech Republic's main COVID-19 testing laboratories, to shut down its computers during the early pandemic; urgent operations were postponed and new acute patients sent elsewhere. Attribution: unattributed		Healthcare IT News: Cyberattack on Czech hospital forces tech shutdown during coronavirus outbreak Brno Daily: Serious cyber-attack targets Brno University Hospital
Kettering Health, 2025 20 May 2025	Ransomware took down Kettering Health's internal systems, phone lines and electronic health records across its Ohio medical centres for more than two weeks; elective procedures were cancelled, some ambulances diverted, and scammers phoned patients pretending to be the hospital. Attribution: Interlock ransomware group (criminal)		The Record: Kettering Health confirms Interlock ransomware attack Healthcare IT News: Kettering Health faces ransomware attack and confirms scam targeting patients