Global Classification of Health Information Systems as Critical, Protected, or High-Security Infrastructure

A comparative study

(updated through January 2026)

Version 1.0

January 2026

Dr Vivek Gupta, MD, MSc

Addl. Prof. and CISO, AIIMS, New Delhi

Comparative analysis of **17 jurisdictions** with detailed chapter coverage,
plus **20+ countries** surveyed across Latin America, ASEAN, Africa, Middle East, and Central Asia

Executive Summary

This comparative study analyzes how **17 jurisdictions** classify health-related information systems and operators as critical infrastructure, plus an additional **20+ countries** surveyed across Latin America, ASEAN, Africa, the Middle East, and Central Asia. Whether framed as *critical information infrastructure*, *critical entities*, *essential services*, or equivalent constructs, this report identifies global patterns and actionable insights for policymakers.

Scope of Analysis

Coverage	Count	Regions
Deep-dive chapters	17	North America, Europe, Asia-Pacific, Middle East
Multi-region survey	20+	Latin America, ASEAN, Africa, Central Asia, Eastern Europe

Key Findings

1. **Universal prioritization of life-and-safety digital functions.** Across all 17 jurisdictions, consistent prioritization emerges for: emergency dispatch systems, major hospital clinical platforms (EMR/EHR, ICU monitoring), blood and organ allocation services, disease surveillance systems, and national health information exchanges.
2. **Multiple designation models, converging on hybrids.** Approaches include:
   - **Sector-based** (USA, Canada): broad coverage, lower precision
   - **Entity-based** (UK, EU, France): clear accountability, scalable
   - **System-based** (Singapore): precise, but complex to administer
   - **Asset-based** (Australia, Germany): explicit thresholds, easy to verify
   - **Hybrid models** increasingly common: combining quantitative thresholds with qualitative "safety net" criteria
3. **Criteria public; lists often confidential.** Most regimes publish designation *criteria* (enabling self-assessment) while keeping specific entity lists confidential to avoid creating target lists. **Exception:** South Korea publishes designations in the Official Gazette.
4. **Tiering structures vary.** From binary (designated/not) to multi-tier:
   - **Two-tier:** EU NIS2 (Essential/Important), Hong Kong (Category 1/2/3 obligations)
   - **Three-tier:** Israel (Basic/Medium/High database security)
   - **Single-tier + enhanced:** Australia (Critical Hospital → SoNS)
5. **2025–2026: A regulatory inflection point.** Eleven major regulatory milestones across eight jurisdictions are entering force, with convergence toward 24-hour early warning and 72-hour detailed incident reporting.

Key Regulatory Milestones (2025–2026)

Date	Jurisdiction	Milestone	Health Sector Impact
1 Apr 2025	Switzerland	Cybersecurity Ordinance (CSV) in force	24h reporting for hospitals, labs
30 May 2025	Australia	Ransomware payment reporting mandatory	Applies to critical hospitals
14 Aug 2025	Israel	Privacy Protection Law Amendment 13	3-tier database security levels
24 Sept 2025	Taiwan	Revised Cyber Security Management Act	MoDA as competent authority
1 Oct 2025	Norway	Digital Security Act in force	Health as "socially important service"
Nov 2025	UK	Cyber Security Bill introduced	Expands to MSPs, 24h reporting
6 Dec 2025	Germany	NIS2 implementation law in force	30,000-case hospital threshold
1 Jan 2026	Hong Kong	CI Ordinance in force	12h/48h/14d incident reporting
1 Jan 2026	Australia	Strict enforcement posture begins	Enhanced supervision of ICU hospitals
May 2026	USA	CIRCIA final rule expected	72h incident/24h ransom reporting
17 July 2026	EU	CER Directive deadline	All-hazard resilience for health

Incident Reporting: Global Convergence

Reporting Stage	Emerging Standard	Jurisdictions
Early warning	12–24 hours	Hong Kong (12h), Norway (24h), Switzerland (24h), EU NIS2 (24h), UK (24h)
Detailed notification	48–72 hours	Hong Kong (48h), Norway (72h), EU NIS2 (72h), USA CIRCIA (72h)
Final report	14–30 days	Hong Kong (14d), Norway (1 month), EU NIS2 (1 month)
Ransom payment	24 hours	USA CIRCIA, Australia

Designation Models (Taxonomy)

Model	Description	Examples
System-based	Specific systems designated	Singapore (CII)
Entity-based	Operators/providers designated	UK (OES), EU (NIS2), France (OIV)
Asset-based	Specific facilities designated	Australia (ICU hospitals), Germany (30k cases)
Sector-based	Obligations apply to classes	USA (HPH sector), Canada (10 CI sectors)
Hybrid	Combined approaches	Germany (KRITIS + NIS2), Hong Kong

Health Entities Most Commonly Designated

Near-universal inclusion (80%+ of frameworks):

- Hospitals with ICU/emergency capability
- National/regional health information exchanges
- Blood and organ allocation services
- Disease surveillance systems
- Emergency ambulance dispatch (CAD)

Frequently included (50–80%):

- Medical laboratories (reference/diagnostic)
- Pharmaceutical manufacturers/distributors
- Medical device manufacturers

Evidence Labels

Where this report lists systems "most likely" to be treated as critical:

- **(A) Explicit** — directly stated in law/regulation

- **(B) Guidance** — stated in official policy documents

- **(C) Criteria inference** — inferred from published thresholds

- **(D) Expert judgement** — reasoned where sources are incomplete

Methodology

This analysis synthesizes:

- Official legislation and regulations (updated through January 2026)
- Competent-authority guidance documents and consultation papers
- Primary source verification for all 17 deep-dive jurisdictions
- Multi-region survey based on official government and agency sources

All substantive claims are supported by numbered references. Where lists are confidential, the report distinguishes between what is directly evidenced and what is inferred.

Table of Contents

Contents

Methodology

identifying, extracting, shortlisting, and categorising "highest-critical / protected" health information systems

This chapter documents the **repeatable method** used to identify country frameworks, extract only verifiable requirements, shortlist what qualifies as "highest critical / protected," and categorise regimes consistently across jurisdictions (as applied in the country chapters already produced).

1) Objective and unit of analysis

Objective: Determine, for each jurisdiction, the **highest critical / protected categories** that can apply to the **health sector and/or health information systems**, and document:

- the **exact legal/regulatory trigger** (definition + threshold test),
- any **tiering / grading scheme**,
- **incident reporting triggers + deadlines**, and
- what is **explicitly health-specific** vs **cross-sector but applicable to health**.

Unit of analysis: Always record what the instrument legally regulates:

- **Entity-level** classification (e.g., "essential entity" vs "important entity"), or
- **Asset/system-level** designation (e.g., "designated system/installation"), or
- **Sector-level** recognition (e.g., "health as a critical sector") when no designation mechanism exists.

2) Evidence hierarchy (what counts as "primary")

To meet a strict evidence standard, sources are ranked and used in this order:

1. **Primary legal texts** (acts, regulations, directives, annexes/schedules, official compilations).
2. **Official regulator/government guidance** that is explicitly issued under, or directly interprets/implements, the primary instrument (e.g., competent authority guidance containing reporting thresholds).
3. **Official explanatory materials** (explanatory memoranda/notes, government bill notes) used only to explain **what the law states**, not to invent new thresholds.
4. **Secondary sources** (law firm notes, academic papers, blogs) are **not used to assert obligations** unless the underlying primary text is also captured; if referenced, they are labelled as secondary.

Hard rule: If a cited document cannot be accessed/verified in full text, it is **not used** to support a factual claim; it is listed as **"not accessible in this environment"** (transparency note).

3) Source discovery and retrieval workflow

For each jurisdiction:

1. **Start from the canonical portal** for legislation (e.g., official gazette/legislation website, EUR-Lex, etc.).

2. Identify the **top instrument(s)** that create "critical/essential" obligations:
   - cybersecurity/critical infrastructure statute,
   - sectoral implementing regulation,
   - annexes/schedules that contain **sector lists** or **numeric thresholds**.
3. Retrieve **competent authority guidance** only where it contains *operational tests* (e.g., explicit "significant incident" thresholds, reporting routes).
4. Capture **version and date** (consolidation date, amendment date, entry into force date) for each instrument.

4) Extraction template (what we extract from each source)

For every instrument, extract only text that supports one of the following fields:

A. Final category (the legal label)

- Exact legal term(s): e.g., "critical infrastructure installation," "operator of essential services," "designated critical information infrastructure," etc.

B. Trigger criteria

- **Definition clause** (what the category is).
- **Threshold test** (numeric or qualitative; annex/schedule thresholds where available).
- **Designation mechanics** (who designates; notice; duration; confidentiality of registers, if stated).

C. Tiering / grading

- Binary vs tiered system; the legal names of tiers; annex references.

D. Incident reporting tests

- Trigger term used by law/guidance ("significant incident," "covered incident," etc.).
- Deadlines (24h/72h/other) and the legal basis for the clock.

E. Health-specific hooks

- Where health is **explicitly named** as a sector/service (or where "medical services," "healthcare providers," "hospitals," etc. appear in annexes).

F. Public vs confidential

- Only recorded if the instrument explicitly states registry confidentiality / publication requirements.

5) Shortlisting logic (inclusion / exclusion)

Inclusion criteria (a framework is shortlisted if it meets any of the following)

1. The legal text **explicitly names health/medical services** as a critical/essential sector/type; **or**
2. The legal text creates a **designation category** that clearly can include health systems by function (e.g., "essential service" including public health) and the health mapping is explicitly present in annex/guidance; **or**

3. The instrument imposes **incident reporting/security obligations** on regulated entities/systems and health entities are explicitly in-scope.

Exclusion criteria (do not include as "highest critical/protected" category)

1. General cybersecurity or data protection obligations **without a "critical/essential" scoping mechanism** (i.e., applies to everyone equally).
2. Voluntary strategies/whitepapers without binding designation tests or mandatory obligations.
3. Purely operational best-practice documents **not anchored** to an identified legal/regulatory regime.
4. Secondary commentary that cannot be traced to accessible primary text.

6) Categorisation scheme used across countries (normalisation)

To compare jurisdictions consistently, each country is categorised along **two orthogonal axes**:

Axis 1 — What is classified

- **Entity-based regimes** (regulated organisations): e.g., essential/important entities.
- **Asset/system-based regimes** (designated installations/systems): e.g., designated CII, KRITIS installations, designated systems.
- **Sector-based framing** (health as a CI sector, but without a public designation list).

Axis 2 — How inclusion is triggered

- **Explicit sector listing** (health/medical named in annex/sector list).
- **Threshold-based** (numeric thresholds like bed counts/case volumes/customers served).
- **Designation-based** (authority determination/notice, often non-public lists).
- **Consequence-based overrides** ("regardless of size" / "significant public health impact" triggers).

This normalisation enables consistent comparison even when countries regulate different objects (entities vs assets).

7) Quality assurance and "zero-interpretation" controls

To keep the output strictly evidentiary:

- **Every factual claim is tied to a citation** (act/regulation clause, annex, or competent authority guidance).
- Any inference is either:
    - **not made**, or
    - clearly labelled as **interpretation** and separated from the "evidence-only" core (depending on the document's rules; for strictest mode, interpretations are omitted).
- **Cross-check dates** (amendment/entry into force) against official sources.
- Maintain a **change log**: if new PDFs are supplied, update only the portions affected and record what changed.

8) Handling language and translation

- Prefer **official English translations** where available (official ministries, EUR-Lex English, etc.).
- If only local-language law is available, extract from:
  - official consolidated text, and
  - reputable official/semiofficial translations where explicitly identified.
- Do **not** "fill gaps" with guessed translation; instead record the limitation.

9) Known limitations (explicitly documented)

- Some regimes intentionally keep **designation lists non-public**; in such cases, the methodology can document **the designation test** and **the secrecy rule**, but cannot confirm named systems/operators from public sources.
- Where official portals block access (e.g., technical/geoblocking), the chapter notes the access limitation and relies only on alternative official materials that were successfully retrieved.

UNITED STATES OF AMERICA (USA)

Final category

Healthcare and Public Health (HPH) Sector — one of the U.S. **Critical Infrastructure Sectors**.

In the U.S. model, this is primarily a **sector-level classification** (not a single public "designated list" of health information systems).

What is "classified" or "designated" in practice?

1) Sector classification (public)

CISA describes U.S. Critical Infrastructure as organized into multiple sectors; **Healthcare and Public Health** is one of them.

2) Entity/asset scoping for incident reporting (developing, rule-based)

Under **CIRCIA**, reporting obligations apply to **"covered entities"** in critical infrastructure (as further defined by rulemaking). The law sets **reporting timelines** (e.g., covered cyber incidents and ransomware payments) but the exact boundary of "covered entity" is operationalized through regulation.

Exact criteria used (as expressed in the cited U.S. materials)

A) Sector boundary (HPH scope)

The HPH sector includes both **public health** and **healthcare** functions/services (sector overview framing).

B) Criticality logic that drives "what systems matter most" (functional dependence)

The HPH Sector-Specific Plan notes that the sector **depends on vast, complex information technology systems** and the **rapid, secure transmission and storage of large amounts of data**—a direct rationale for treating key health information systems as high-impact from a resilience/security perspective.

C) CIRCIA reporting thresholds (obligation trigger)

CIRCIA sets statutory reporting clocks: **covered cyber incidents** must be reported **within 72 hours**, and **ransomware payments within 24 hours** (as summarized in the fact sheet).

Is there grading / tiering of "criticality" for health information systems?

The U.S. approach is expressed more as:

- a **sector construct** (HPH as a CI sector), and
- **reporting/obligation scoping** via CIRCIA's "covered entity / covered incident" framework,

rather than an explicit **public tiering scheme** that assigns every health information system to a graded level.

However, CISA operational publications do show **risk-impact thinking** (e.g., protection goals like availability/integrity for "critical HPH systems, functions, and data").

What is public vs confidential?

Public * The fact that HPH is a **Critical Infrastructure Sector** is public. * High-level reporting obligations and timelines under CIRCIA are public (as summarized by CISA).

Potentially non-public / organization-specific * Exact lists of which specific hospitals/entities/systems are most critical in a given locality or network are typically handled through **risk management and coordination**, rather than a single universal public register in the materials provided. * RVA-type findings are published in anonymized form; the advisory describes the engagement and outcomes without naming the organization.

Which *health information systems* are most likely to be treated as "highest criticality" in the U.S. framing?

CISA sector documents and advisories emphasize **mission-essential functions**, **data dependence**, and **operational disruption patterns**. Consequently, the "highest criticality" systems in the health sector typically cluster into these categories:

1) Care-delivery operational systems (availability-critical)

Systems whose loss disrupts direct patient care delivery and continuity: * Core clinical workflow platforms and associated identity/access dependencies (because HPH depends on large, complex IT and rapid/secure data flows).

CISA's mitigation guide is explicit that threats can affect **critical HPH systems, functions, and data** and highlights patient-focused service impacts as a central concern.

2) Public-health coordination and information flows (societal-impact critical)

Systems enabling public health operations and situational awareness—because the sector's planning and operations depend on **information sharing and data**. The SSP explicitly frames dependency on secure transmission/storage at scale.

3) Enterprise IAM / domain services and internal network controls (blast-radius critical)

CISA's RVA advisory shows that once an attacker is "inside," **misconfigurations/weak passwords** can enable **domain compromise**, and it highlights actions like **phishing-resistant MFA for administrative access**, removing default credentials, and **network segregation**—all pointing to IAM/domain control planes as high criticality in health enterprises.

4) Vulnerability/patch posture for legacy and exposed systems (exploitability critical)

The same RVA advisory documents issues such as weak password policy and stresses the importance of stronger credential hygiene (e.g., longer passwords), patching, and segregation when patching is not possible—patterns highly relevant to clinical environments with legacy platforms and constrained devices.

5) Ransomware resilience dependencies (operational continuity critical)

The ransomware advisory for HPH explicitly frames ransomware as an operational disruption problem for the sector—driving prioritization of systems needed for continuity of care and contingency operations.

Practical "tests" (derived from the U.S. documents)

A health information system in the U.S. context is most plausibly "high criticality / highest security priority" if it satisfies one or more of these document-grounded tests:

1. **IT-dependence test:** It is part of the "vast, complex" IT environment required for healthcare delivery and for rapid, secure data movement/storage at scale.
2. **Service disruption test:** Its compromise materially affects "critical HPH systems, functions, and data," especially patient-focused service continuity.
3. **Enterprise blast-radius test:** Its compromise enables broad takeover (e.g., domain compromise) or bypass of administrative control—highlighted by CISA's RVA outcomes and recommended mitigations (phishing-resistant admin MFA, default credential removal, segregation).
4. **Regulatory reporting relevance test (CIRCIA):** Incidents affecting it are more likely to be "covered cyber incidents" (depending on final covered-entity definitions) and therefore time-bound reporting obligations (72h/24h) become operationally relevant for the owning organization.

References (USA)

1. **CISA — Critical Infrastructure Sectors** (includes Healthcare and Public Health as a sector). (CISA)
2. **CISA — Healthcare and Public Health Sector** (sector overview framing). (CISA)
3. **NIPP Sector-Specific Plan: Healthcare and Public Health (2015)** — dependency on complex IT and rapid/secure data flows. (CISA)

4. **CISA — CIRCIA Fact Sheet (2022)** — 72-hour covered incident reporting and 24-hour ransomware payment reporting timelines. (CISA)
5. **CISA — AA23-349A: HPH Sector Risk & Vulnerability Assessment** — internal weaknesses leading to domain compromise; recommended mitigations. (CISA)
6. **CISA — AA20-302A: Ransomware Activity Targeting the HPH Sector** — operational disruption framing for HPH ransomware. (CISA)

AUSTRALIA

Final categories (what the law actually classifies)

1. **Critical infrastructure asset (health care and medical sector): "critical hospital"** — a **hospital that has a "general intensive care unit"**. (Federal Register of Legislation)
2. **CIRMP in-scope subset: "designated hospital"** — **a critical hospital mentioned in Schedule 1** of the **Critical infrastructure risk management program Rules (LIN 23/006)**; **Part 2A (CIRMP)** applies to a designated hospital. (Federal Register of Legislation)
3. **Higher-tier classification: "system of national significance (SoNS)"** — the Act creates **Enhanced cyber security obligations** (Part 2C) that operate **in relation to systems of national significance**, including statutory incident response planning obligations and related requirements. (Federal Register of Legislation)

Exact legal / regulatory criteria (what triggers inclusion)

A) "Critical hospital" (health CI asset trigger)

- **Definition (Act):** "critical hospital means a hospital that has a general intensive care unit." (Federal Register of Legislation)
- **"General intensive care unit" definition (Act):** the Act defines what qualifies as a "general ICU" (capable of mechanical ventilation for several days and invasive cardiovascular monitoring, with specified specialist support). (Federal Register of Legislation)
- **Sector mapping (Act):** "a critical hospital is taken to relate to the health care and medical sector." (Federal Register of Legislation)
- **Critical infrastructure asset listing (Act):** "critical hospital" is included in the Act's definition/listing of **critical infrastructure assets**. (Federal Register of Legislation)

B) "Designated hospital" (CIRMP / Part 2A trigger)

- **Definition (Rules):** "designated hospital means a critical hospital mentioned in Schedule 1." (Federal Register of Legislation)
- **Part 2A application (Rules):** for the Act's Part 2A application provision, the Rules specify that **Part 2A applies to… (g) a designated hospital**. (Federal Register of Legislation)

C) SoNS (Enhanced cyber security obligations trigger)

- **Enhanced cyber security obligations exist in the Act** (Part 2C), and are expressly framed as relating to **systems of national significance**. (Federal Register of Legislation)
- **Example of SoNS-linked obligation (Act):** the Act sets out SoNS-related requirements around **incident response plans** (including compliance, review, update, and provision to the Secretary), and specifies that an incident response plan for a SoNS must relate to cyber security incidents and plan for responding to incidents with relevant impact. (Federal Register of Legislation)

Grading / tiering schemes (what is explicit vs not)

What is explicit in instruments (evidentiary):

- **Binary at the asset layer:** "critical hospital" is the health-sector CI asset class in the Act. (Federal Register of Legislation)
- **CIRMP step-up:** "designated hospital" is a defined subset, and the Rules explicitly apply Part 2A (CIRMP) to it. (Federal Register of Legislation)
- **Further step-up exists for SoNS:** the Act explicitly provides an additional layer of obligations under Part 2C for systems of national significance. (Federal Register of Legislation)

What is *not* explicit (and should not be asserted as fact):

- The law does **not** publish a universal "Tier 1/2/3" label scheme for hospitals; any "tiering" language is a **presentation convenience** rather than a statutory classification.

Health information systems most likely treated as "high criticality" in practice

Interpretation (not a direct statutory list): The SOCI framework designates **assets (hospitals / SoNS systems)** rather than enumerating specific hospital IT systems. However, the **CIRMP Rules** define **"cyber and information security hazard"** in terms of improper access/misuse of information or computer systems related to the CI asset, or use of computer systems to obtain unauthorised control/access that might impair functioning. (Federal Register of Legislation) **Interpretation (supported by the obligation scope above):** for **critical hospitals / designated hospitals**, systems that are tightly coupled to delivering the hospital's critical functions (and whose compromise would plausibly "impair its proper functioning") are the ones most likely to be operationally prioritised under CIRMP cyber/information security hazards (e.g., core clinical and operational platforms). (Federal Register of Legislation) **Additional evidentiary hook (Rules):** the Rules explicitly note that **a data storage system** meeting requirements under **subsection 9(7) of the Act** for an in-scope CI asset is **taken to be part of the CI asset**, and include "material risk" examples referencing impacts to ICT/OT and to **data storage systems holding business critical data**. (Federal Register of Legislation)

Public vs confidential (what is public, what is not)

- **Public (criteria/instruments):** the Act and the CIRMP Rules (including the definition of "designated hospital" and the fact Schedule 1 exists) are published. (Federal Register of Legislation)
- **Register / lists not public (Act):** the Act provides that the Secretary must keep a Register and **"must ensure that the Register is not made public."** (Federal Register of Legislation)

References (Australia)

1. **Australian Government — Federal Register of Legislation.** *Security of Critical Infrastructure Act 2018* (Compilation incl. definitions of "critical hospital" and "general intensive care unit"; health-sector mapping; register confidentiality; Part 2B/2C structure; SoNS-related obligations). (Federal Register of Legislation)

2. **Australian Government — Federal Register of Legislation.** *Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023* (Compilation 04 Apr 2025: definition of "designated hospital"; Part 2A application to designated hospitals; definition of cyber/information security hazard; data storage system note; material risk examples). (Federal Register of Legislation)

EUROPEAN UNION (NIS2)

Legal basis

Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union ("NIS2"). ([EUR-Lex](#))

Final Categories (what the Directive actually creates)

1) Essential entities

NIS2 defines **"essential entities"** in **Article 3(1)** (including Annex I entities above the "medium-sized" ceiling, plus several additional categories). ([EUR-Lex](#))

2) Important entities

Entities in scope that **are not essential** are **"important entities"** under **Article 3(2)**. ([EUR-Lex](#))

Exact legal / regulatory criteria

Step 1 — Is the entity in an Annex I or Annex II type?

NIS2 applies to **public or private entities of a type referred to in Annex I or II** (subject to the scope rules below). ([EUR-Lex](#))

Step 2 — Size-based scope rule (default rule)

By default, NIS2 applies to Annex I / Annex II entities that **qualify as medium-sized enterprises** (per EU SME Recommendation) **or exceed the medium-sized ceilings**, and that provide services/carry out activities in the Union. ([EUR-Lex](#))

Step 3 — "Regardless of size" triggers (explicit in Article 2(2)–(4))

Even if below the medium-sized threshold, the Directive **also applies regardless of size** to Annex I/II entities where (among others):

- the entity is the **sole provider** in a Member State of an essential service, **or**
- disruption could have a **significant impact** on **public safety / public security / public health**, **or**
- disruption could induce a **significant systemic risk** (including cross-border impact), **or**
- the entity is critical due to **specific importance at national/regional level** for a sector/service or interdependent sectors. ([EUR-Lex](#))

Also: **entities identified as critical entities under Directive (EU) 2022/2557** fall within scope regardless of size (Article 2(3)). (EUR-Lex)

Step 4 — Essential vs Important classification (Article 3)

- **Essential** includes (a) **Annex I** entities that exceed the medium-size ceilings, plus other listed categories (and Member State identifications under Article 2(2)(b)–(e)). (EUR-Lex)
- **Important** = Annex I/II entities that are in scope but **do not qualify as essential**. (EUR-Lex)

Health sector coverage

Annex I (Essential-sector types) — Health

Annex I includes a **Health** sector with: * **Health care providers**, and * **EU reference laboratories**. (EUR-Lex)

Annex II (Important-sector types) — Health-adjacent manufacturing

Annex II includes manufacturing categories that cover (among others):

- **medical devices**,
- **in vitro diagnostic medical devices**, and
- **medicinal products**. (EUR-Lex)

  Interpretation (explicitly marked): NIS2's legal "final categories" are **entity categories** (essential/important). It does **not** itself publish a list of "critical systems" in healthcare; instead it places obligations on the **in-scope entity**, and those obligations practically attach to the network & information systems used to provide the covered services.

Grading / tiering schemes

NIS2's formal structure is a **two-tier classification**: **Essential** vs **Important**. (EUR-Lex) It also contains **explicit "regardless of size" inclusion tests** (sole provider / public health impact / systemic risk / special national or regional importance), which function as legal "criticality overrides" for inclusion in scope. (EUR-Lex)

Incident reporting (exact timings in the Directive)

For **significant incidents**, Member States must ensure entities submit:

- **Early warning**: **within 24 hours** of becoming aware. (EUR-Lex)
- **Incident notification**: **within 72 hours** of becoming aware. (EUR-Lex)
- **Final report**: **no later than one month** after the incident notification (with additional progress/final timing for ongoing incidents). (EUR-Lex)

NIS2 also contains a clause allowing authorities, after consulting the entity, to **inform the public** or require the entity to do so where public awareness is necessary / in the public interest. ([EUR-Lex](#))

Lists and transparency (what is mandated vs not mandated)

List requirement (mandated)

By **17 April 2025**, Member States must **establish a list** of essential and important entities (and review/update at least every two years). ([EUR-Lex](#)) Entities must submit minimum identifying information (name, address/contact, sector/subsector, Member States where services are provided). ([EUR-Lex](#))

Publication of the list (not mandated in the text shown)

In the provisions cited above, NIS2 **requires a list to exist** and prescribes information flows (including statistical reporting to the Commission), but it does **not** state that Member States must publish a public registry. ([EUR-Lex](#)) It also explicitly addresses confidentiality constraints on information exchange (confidential business information, etc.). ([EUR-Lex](#))

Interpretation: mapping to "health information systems most likely classified"

*(These are examples to help operationalize the entity-scoped law; they are **not** lists from NIS2 itself.)* If a **hospital / clinic / health care provider** is in-scope as an essential/important entity, then systems typically implicated will include (as an operational matter): EHR/EMR platforms, PAS, ED/ICU/OR systems, LIS, RIS/PACS, pharmacy/medication systems, blood bank/transfusion systems, identity/access, and supporting infrastructure used to deliver the service. If **EU reference laboratories** are in-scope, then their surveillance/diagnostic IT (e.g., LIMS and associated data flows) are the most obvious in-scope systems. If **medical device / IVD / medicinal product manufacturers** are in-scope (Annex II), then manufacturing/quality systems and supporting enterprise IT used to produce/release products are the most obvious in-scope systems.

References (European Union)

1. **Directive (EU) 2022/2555 (NIS2 Directive)** — Official Journal of the European Union (EUR-Lex PDF). ([EUR-Lex](#))

CANADA

Final category

Canada's top-level framing for "critical / protected" health systems is **sector-based**:

1. **Critical Infrastructure (CI) — "Health" sector** (one of **10** CI sectors in Canada's National Strategy / Public Safety Canada CI framework). (Public Safety Canada)
2. **Federally regulated "critical cyber systems" (designation-based obligations) — via Bill C-8 / proposed CCSPA framework** for **designated operators** of certain **vital services/systems** within Parliament's jurisdiction (not a "health CI designation list," but relevant to cross-cutting dependencies such as telecom, energy/pipelines, transport, banking/clearing). (Ministère de la Justice)

Exact legal / policy criteria used

A) National Critical Infrastructure (Public Safety Canada) — public definition + sector model

CI definition (public): CI refers to "processes, systems, facilities, technologies, networks, assets and services" essential to Canadians' health/safety/security/economic well-being and the effective functioning of government. (Public Safety Canada)

Sector list (public): The National Strategy enumerates **ten CI sectors**, explicitly including **Health**. (Public Safety Canada)

How inclusion works (important): This is a **resilience / partnership framework**, not a single national law that publishes a universal, named list of "designated health information systems." The Strategy emphasizes:

- **shared responsibilities** across federal/provincial/territorial governments, local authorities, and owners/operators, with owners/operators bearing primary responsibility for protecting assets/services; (Public Safety Canada)
- an **all-hazards risk management approach** and improved **information sharing/protection** among partners. (Public Safety Canada)

B) Federal designation-based cyber obligations (Bill C-8 / CCSPA concept)

What CCSPA would do (as described by Justice Canada):

- **Part 2** would enact the **Critical Cyber Systems Protection Act (CCSPA)** to protect "critical cyber systems" supporting **vital services/systems** within Parliament's jurisdiction that are vital to national security or public safety. (Ministère de la Justice)
- It would authorize designation of **classes of operators ("designated operators")** who own/control/operate critical cyber systems; these operators would have specified obligations. (Ministère de la Justice)
- "Vital" systems/services initially include sectors such as **telecommunications**, **pipelines/power lines**, **nuclear energy**, **transportation**, **banking** and **clearing/settlement**, with potential additions by Governor in Council. (Ministère de la Justice)

Bill text purpose clause (primary text): the purpose is to protect critical cyber systems to support continuity/security of vital services/systems, including managing cyber risks (incl. supply chain/third-party), protecting systems from compromise, detecting incidents, and minimizing impacts. (Parliament of Canada)

Grading / tiering scheme

Canada's CI model is primarily **sector-in-scope** (e.g., "Health" as a CI sector) rather than a published graded tiering of all health information systems. (Public Safety Canada)

Under the CCSPA approach (if enacted), the main "tier" is **designation status**:

- **designated operator** vs **non-designated operator** (federally regulated vital service/system operators). (Ministère de la Justice)

"Higher security" triggers relevant to health (what becomes critical in practice)

Because Canada's national CI approach is sector + consequence + interdependency (rather than a single national list), the most "critical / higher-security" health systems are typically those whose disruption plausibly causes:

- **loss of vital services** or **harm / loss of life**, which Cyber Centre CI guidance highlights as potential CI impacts; (Canadian Centre for Cyber Security)
- **hospital operational disruption** / compromised medical devices (explicitly called out as a CI cyber-impact risk). (Canadian Centre for Cyber Security)

This supports prioritizing, in practice (examples, not an official list): core hospital operational platforms, emergency workflows, key diagnostic and medication systems, public health coordination platforms, and enterprise identity/network controls that have wide "blast radius."

Public vs confidential

Public

- CI definition and the **10-sector list including Health** are explicitly public. (Public Safety Canada)
- Federal legislative instruments (Bill text, Charter Statement, legislative summaries) are public. (Parliament of Canada)

Typically not public (operational practice)

Specific, organization-level inventories of "most critical" systems (within hospitals/provinces/health authorities) are generally managed via risk management and operational security processes implied by the partnership/owner-operator responsibility model, rather than published as a single universal national register in the cited framework. (Public Safety Canada)

Latest updates (strictly sourced)

- **Public Safety Canada CI overview page** shows update metadata (Jan 2025) and reiterates CI definition + the 10 sectors including Health. (Public Safety Canada)
- **Cyber Centre CI guidance page** shows update metadata (Jul 2025) and reiterates CI definition, sector list, and CI cyber impacts. (Canadian Centre for Cyber Security)
- **Bill C-8 (45th Parliament, 1st session)**: LEGISinfo lists the bill and links to the bill text and Charter Statement. (Parliament of Canada)
- **Library of Parliament legislative summary (PDF)** notes CCSPA incident reporting requirements for designated operators, including a reporting period that "cannot exceed 72 hours" for reporting certain incidents to CSE. (Parliamentary Library of Canada)

References (Canada)

1. **Public Safety Canada — *National Strategy for Critical Infrastructure*** (sector list, CI definition, partnership/all-hazards/info sharing model). (Public Safety Canada)
2. **Public Safety Canada — *Canada's Critical Infrastructure (CI)*** (CI definition; 10 sectors including Health). (Public Safety Canada)
3. **RCMP — *Safeguarding critical infrastructure*** (10 sectors list including Health). (RCMP)
4. **Canadian Centre for Cyber Security — *Security considerations for critical infrastructure (ITSAP.10.100)*** web page (CI definition; sector list; CI impacts and mitigations context). (Canadian Centre for Cyber Security)
5. **Canadian Centre for Cyber Security — *ITSAP.10.100 PDF*** (threats, impacts including hospital operations/medical devices; CI definition). (Canadian Centre for Cyber Security)
6. **Parliament of Canada — *LEGISinfo: Bill C-8*** (bill listing, links to text + Charter Statement + legislative summary). (Parliament of Canada)
7. **Parliament of Canada — *Bill C-8 (First Reading text)*** (purpose clause for protecting critical cyber systems). (Parliament of Canada)
8. **Justice Canada — *Charter Statement: Bill C-8*** (Part 2 enacts CCSPA; designated operators; initial vital services list). (Ministère de la Justice)
9. **Library of Parliament — *Legislative Summary of Bill C-8 (PDF)*** (incident reporting requirement summary, including period not exceeding 72 hours). (Parliamentary Library of Canada)

UNITED KINGDOM (UK)

Final categories (what is "highest critical / protected" in this regime)

1. **Operator of Essential Services (OES) — Health (England)**

- The DHSC health-sector guide states that **"Healthcare services are an essential service under the NIS Regulations"** and that **"NHS trusts and foundation trusts, integrated care boards (ICBs) and certain independent providers [are] currently designated OESs for healthcare services."** (GOV.UK)
- The same guide states that **the Secretary of State for Health and Social Care, acting through DHSC, is responsible for overseeing the NIS Regulations for OESs within the health sector in England** (i.e., DHSC is the competent authority for the England health sector). (GOV.UK)

2. **Relevant Digital Service Provider (RDSP) — cross-sector category (often relevant to health supply chains)**

- The ICO's Guide to NIS is explicitly for organisations providing digital services such as **online marketplaces, online search engines and cloud services**, and it explains RDSP obligations and the ICO's role as the UK competent authority for RDSPs. (ICO)
- The **NIS Regulations 2018** define **"digital service"** as including **(a) online marketplace, (b) online search engine, (c) cloud computing service**, and define **"cloud computing service."** (Legislation.gov.uk)

3. **Proposed expansion (Bill introduced 12 Nov 2025 — Bill 329)**

- The **Cyber Security and Resilience (Network and Information Systems) Bill** explanatory notes (within the Parliament PDF) describe new/expanded regulated roles including **relevant managed service providers (RMSPs)** and **critical suppliers**. (UK Parliament)

Exact legal / regulatory criteria (what triggers inclusion)

A) OES (Health sector, England)

- The DHSC guide states the health-sector OES landscape in England (NHS trusts/foundation trusts, ICBs, and certain independent providers are **currently designated** as OESs for healthcare services). (GOV.UK)
- The DHSC guide states it is published under **regulation 3** guidance duties, and that OESs **must have regard to it** when carrying out security and incident reporting duties under the NIS Regulations. (GOV.UK)

B) RDSP (ICO-regulated)

- The DHSC guide lists criteria for being an RDSP (all must apply), including providing an online search engine/online marketplace/cloud computing service in the UK; UK head office or nominated UK representative; and not being a micro/small enterprise (staff/turnover thresholds). (GOV.UK)

- The ICO states its guide summarises obligations for **RDSPs** and explains the ICO's role as competent authority for RDSPs. (ICO)

Incident reporting tests and thresholds (evidence only)

OES (Health, England) — "significant impact" + DHSC Table 1 thresholds

- The DHSC guide states that OES reports must be submitted **via the Data Security and Protection Toolkit (DSPT) without undue delay and, in any event, no later than 72 hours** after the OES became aware that an NIS incident has occurred. (GOV.UK)
- The DHSC guide states OESs must assess significance having regard to **(i) number of users affected, (ii) duration, (iii) geographical area**, and provides **Table 1 thresholds** for the health sector definition of significant impact. (GOV.UK)

Examples of explicit Table 1 thresholds (DHSC):

- **Excess fatalities:** > 0; **Potential clinical harm:** > 50 patients at risk. (GOV.UK)
- **ED closure/diversion:** > 3 hours (major trauma centre); > 24 hours (all other organisations). (GOV.UK)
- **Outpatient appointments cancelled:** 1,500; **Inpatient episodes cancelled:** 250. (GOV.UK)
- **NHS111 services unavailable:** > 3 hours. (GOV.UK)

RDSP (ICO) — 72-hour reporting requirement

- The ICO states: **notify the ICO without undue delay and not later than 72 hours** of becoming aware of any incident (where feasible). (ICO)
- The ICO also states: **only RDSPs** notify the ICO; **OESs notify their sector competent authority**. (ICO)

Grading / tiering scheme (as published)

- The regime is **categorical by role** (e.g., **OES** vs **RDSP**) with different competent authorities and obligations, as reflected in the DHSC guide (OES) and ICO guidance (RDSP), and in the NIS Regulations' definitions/structure. (GOV.UK)

Latest updates (2025–2026) — Bill introduced 12 Nov 2025 (Bill 329) (evidence only)

From the Bill's explanatory notes:

- A **two-stage reporting structure** is described: **initial notification within 24 hours** of becoming aware, and **full notification within 72 hours** (described for OES incidents and similarly for RDSP incidents). (UK Parliament)
- The notes also state that regulated entities must **send a copy of notifications to the CSIRT** (NCSC in its CSIRT capacity) **at the same time** as notifying the regulator. (UK Parliament)
- The explanatory notes describe **managed services / RMSPs** and **critical suppliers** as added/expanded regulated categories. (UK Parliament)

References (United Kingdom)

1. **DHSC (GOV.UK):** *The Network and Information Systems Regulations 2018: guide for the health sector in England* (OES scope statement; DHSC oversight; DSPT reporting route; 72 hours; Table 1 thresholds). (GOV.UK)
2. **UK Legislation:** *The Network and Information Systems Regulations 2018 (S.I. 2018/506) — PDF* (definitions of digital service / cloud computing service; RDSP references). (Legislation.gov.uk)
3. **ICO:** *The Guide to NIS* (scope: online marketplace/search/cloud services; ICO role as competent authority for RDSPs). (ICO)
4. **ICO:** *Incident reporting (Guide to NIS)* (RDSP-only notification to ICO; "without undue delay and not later than 72 hours"; NCSC notification suggestion). (ICO)
5. **UK Parliament Publications:** *Cyber Security and Resilience (Network and Information Systems) Bill — Explanatory Notes (Bill 329; introduced 12 Nov 2025)* (24h/72h staged reporting; CSIRT copy; RMSPs/managed services; critical suppliers). (UK Parliament)

GERMANY

Final categories

Germany applies **two distinct, formal classification layers** that can bring health-sector entities/systems into heightened cybersecurity obligations:

1. **KRITIS (Critical Infrastructure) — "Kritische Anlagen" / critical installations (anlagenbezogen)**
   - Instrument: **BSI-Kritisverordnung (BSI-KritisV)** (Verordnung zur Bestimmung kritischer Anlagen nach dem BSI-Gesetz). ([Gesetze im Internet](#))
   - Health sector thresholds are in **Anhang 5 (Sektor Gesundheit)**. ([Gesetze im Internet](#))
2. **NIS2 implementation (entity-based) — "Besonders wichtige Einrichtungen" and "Wichtige Einrichtungen"**
   - Instrument: **BSI-Gesetz (BSIG)** (2025 consolidated version on Gesetze-im-Internet), including sector lists in **Anlage 1** and **Anlage 2**. ([Gesetze im Internet](#))
   - Official statements indicate the **NIS-2 implementation law entered into force on 6 Dec 2025**. ([Bundesregierung](#))

Exact legal / regulatory criteria (how classification is determined)

A) KRITIS (Health sector) — threshold test in BSI-KritisV Anhang 5

A health installation is KRITIS-relevant when it matches an Anlagenkategorie in **Anhang 5** and meets the defined **Schwellenwert**.

Examples explicitly shown in the annex include:

- **Hospitals (Krankenhaus)**: **Vollstationäre Fallzahl/Jahr = 30,000**. ([Gesetze im Internet](#))
- **Labor / lab IT service constellation** (diagnostics/therapy-control IT services for at least one lab): **1,500,000** (threshold shown in the Anhang 5 text snippet). ([Gesetze im Internet](#))
- **Blood/plasma donation control system** (*Blut- oder Plasmaspendensteuerungssystem*): **Hergestellte oder in Verkehr gebrachte Produkte/Jahr = 34,000**. ([Gesetze im Internet](#))

Timing rule (when KRITIS status applies): the BSI-KritisV provides that an installation is treated as KRITIS **from 1 April of the calendar year following** the year in which the threshold is first reached/ exceeded (and ceases similarly after dropping below). ([bmi.bund.de](#))

B) NIS2 (BSIG 2025) — entity/sector test via Anlage 1 & Anlage 2

Under the BSIG consolidated 2025 version, the sector lists in **Anlage 1** and **Anlage 2** are used to classify organisations as:

- **"Besonders wichtige Einrichtungen"** (especially important) and/or
- **"Wichtige Einrichtungen"** (important),

depending on the applicable sector listing and legal framing. ([Gesetze im Internet](#))

Health-relevant entries evidenced in the annexes include:

- **Anlage 1** contains health-related entries such as **pharmaceutical R&D** (in relation to medicines), and references to **medical devices for public-health emergency situations** (linked to EU emergency mechanisms). (Gesetze im Internet)
- **Anlage 2** includes **manufacture of in-vitro diagnostics** and related medical device manufacturing language (as shown in the Anlage 2 snippet). (Gesetze im Internet)

(The evidence above is limited to the retrieved official passages.)

Registration / notification (explicit requirement)

The BSIG includes a **registration obligation**: covered entities must register **no later than three months** and provide required information to the competent system/authority. (Gesetze im Internet)

Grading / tiering scheme (as evidenced)

- **KRITIS (BSI-KritisV):** effectively **binary** at installation level (threshold met vs not met), using **numeric thresholds** in Anhang 5. (Gesetze im Internet)
- **NIS2 (BSIG 2025): two-tier entity categorisation** via **Anlage 1 vs Anlage 2** structure (especially important vs important sectors/entities). (Gesetze im Internet)

Public vs confidential

- **Public:** KRITIS thresholds for health are published in **Anhang 5** (Gesetze-im-Internet), and BSIG sector annexes are also published on Gesetze-im-Internet. (Gesetze im Internet)
- **KRITIS statistics:** BSI publishes KRITIS "in figures" (aggregated reporting). (BSI)

Operational note

Germany's hospital sector uses **B3S (branch-specific security standard) materials** in practice. The DKG's submitted B3S document explicitly references applicability beyond only KRITIS hospitals (e.g., those exceeding **30,000** inpatient cases) and frames B3S usage as an implementation approach in context. (dkgev.de)

References (Germany)

1. **BSI-KritisV** (Gesetze-im-Internet) — regulation index. (Gesetze im Internet)
2. **BSI-KritisV — Anhang 5 (Sektor Gesundheit)** (Gesetze-im-Internet) — hospital threshold 30,000 cases/year (and health sector annex basis). (Gesetze im Internet)
3. **BSI-KritisV — health/lab IT threshold evidence** (Gesetze-im-Internet snippet from Anhang 5 showing 1,500,000). (Gesetze im Internet)
4. **BSI-KritisV — Blut-/Plasmaspendensteuerungssystem threshold 34,000** (Gesetze-im-Internet + PDF snippet). (Gesetze im Internet)
5. **BSI-KritisV timing rule ("ab dem 1. April …")** (BMI PDF + Gesetze snippet). (bmi.bund.de)
6. **BSIG (2025 consolidated)** (Gesetze-im-Internet) + **Anlage 1** + **Anlage 2**. (Gesetze im Internet)

7. **Anlage 1 health-related entries (pharma R&D; emergency medical device linkage)** (Gesetze-im-Internet snippet). ([Gesetze im Internet](#))
8. **Anlage 2 health supply-chain entry (in-vitro diagnostics / medical devices manufacturing snippet)** (Gesetze-im-Internet snippet). ([Gesetze im Internet](#))
9. **BSIG §33 registration obligation ("spätestens drei Monate …")** (Gesetze-im-Internet snippet). ([Gesetze im Internet](#))
10. **Entry into force date (6 Dec 2025) — Federal Government + BSI press release**. ([Bundesregierung](#))
11. **EU Regulation (EU) 2022/123 — Article 22 ("Liste kritischer Medizinprodukte …")** (EUR-Lex PDF). ([EUR-Lex](#))
12. **DKG B3S hospital security standard submission document (2025-07-25)** (PDF). ([dkgev.de](#))

SINGAPORE

Final Categories

Cybersecurity Act (2018; amended 2024)

- **Critical Information Infrastructure (CII)** — a **computer or computer system** designated under **section 7(1)** (i.e., system-level designation, not "whole organisations/sectors"). ([Cyber Security Agency of Singapore](#))

CII sector coverage (policy statement):

- CSA identifies **Healthcare** as one of the critical sectors in scope for CII-protected essential services. ([Cyber Security Agency of Singapore](#))

Exact Legal/Regulatory Criteria (designation test)

Under **section 7(1)** (as described in CSA's official FAQ and the Act's Explanatory Statement), a system may be designated as CII where it is:

1. **Located wholly or partly in Singapore**, and
2. **Necessary for the continuous delivery of an "essential service"**, and
3. The system's **loss or compromise** will have a **debilitating effect on the availability** of that essential service in Singapore. ([Cyber Security Agency of Singapore](#))

"Essential service" framing (why healthcare can qualify): the Explanatory Statement describes "essential service" as a service essential to national-level interests (including **public health**) and **specified in the First Schedule**. ([Isomer User Content](#)) **Designation mechanics and duration:** * Designation is **by written notice** to the system owner. ([Isomer User Content](#)) * Designation takes effect for **5 years** unless withdrawn earlier; CSA explains this as allowing periodic re-evaluation as circumstances change. ([Isomer User Content](#))

Grading/Tiering Schemes

- **No published multi-tier grading** for CII designation — the regime is essentially **designated CII vs non-CII** (with the list of designated CII itself not public). ([Cyber Security Agency of Singapore](#))

Obligations once designated (high-level; from official explanatory material + CSA CII Code)

From the Cybersecurity Act Explanatory Statement, CII owners' duties include (among others):

- comply with **Codes of Practice / Standards of Performance** and directions,
- **report prescribed cybersecurity incidents**,
- undergo **audits at least once every 2 years**,
- perform **cybersecurity risk assessments at least once a year**, and
- participate in **cybersecurity exercises** if required. ([Isomer User Content](#))

CSA publishes the **Cybersecurity Code of Practice for CII (PDF)** under its legislation resources (non-compliance is enforceable via directions under the Act, per the Explanatory Statement). ([Cyber Security Agency of Singapore](#))

Healthcare information systems "most likely" designated CII

Strict evidentiary position (what can be said publicly):

- **CSA states the list of CII and CII owners is secret for national security reasons**, and **CII refers to specific computers/systems explicitly designated** (not "firms and sectors"). Therefore **specific health systems (e.g., NEHR, ED systems, etc.) cannot be confirmed as CII from public sources**. ([Cyber Security Agency of Singapore](#))

Related but not a CII designation list (health sector cyber requirements):

- MOH has issued **Cyber and Data Security Guidelines for Healthcare Providers** in the context of safe contribution/access to **NEHR** (this is a healthcare-sector cyber baseline document, not a publication of CII designations). ([Health Information](#))

Public vs Confidential

Public:

- CSA publicly describes the **CII definition** and **critical sector scope** (including healthcare) and links to CII regulatory materials and Codes of Practice. ([Cyber Security Agency of Singapore](#))

Confidential:

- **The list of CII and CII owners is secret** (CSA's explicit statement). ([Cyber Security Agency of Singapore](#))

Latest Updates (2024–2026) — what can be evidenced from official sources

- CSA states **amendments to the Cybersecurity Act were passed in Parliament in May 2024**, including updates to the CII provisions (and new regulated classes like STCC/ESCI/FDI). ([Cyber Security Agency of Singapore](#))
- CSA's legislation pages show the current published **CII Code of Practice** and its last-updated date on the site. ([Cyber Security Agency of Singapore](#))

References (Singapore)

1. **Cyber Security Agency of Singapore (CSA). FAQs — Cybersecurity Act** (CII definition; sectors; secrecy of CII list; 5-year designation rationale). ([Cyber Security Agency of Singapore](#))
2. **Government of Singapore / CSA. Cybersecurity Act — Explanatory Statement (PDF)** (section-by-section explanation including section 7 test; 5-year effect; duties like audits/risk assessments). ([Isomer User Content](#))

3. **CSA. Cybersecurity Act (overview page)** (notes amendments passed May 2024; sector list including healthcare; links to official sources). (Cyber Security Agency of Singapore)

4. **CSA. Codes of Practice page** (official listing and link to CII Code of Practice PDF). (Cyber Security Agency of Singapore)

5. **CSA. Cybersecurity Code of Practice for Critical Information Infrastructure (PDF)** (detailed CII owner requirements). (Isomer User Content)

6. **Ministry of Health (Singapore). Cyber & Data Security Guidelines for Healthcare Providers (PDF)** (NEHR-linked healthcare provider cyber requirements; not a CII designation list). (Health Information)

JAPAN

Legal Basis

- **Basic Act on Cybersecurity (Act No. 104 of 2014)** — establishes the national cybersecurity policy framework and defines *critical social infrastructure providers* as those providing infrastructure foundational to people's lives/economic activity where failure/deterioration would have enormous impact.
- **Cybersecurity Policy for Critical Infrastructure Protection** (Cybersecurity Strategic Headquarters; June 17, 2022; revised March 8, 2024) — sets the government-wide CIP framework and terminology for CI operators, CI sectors, CI services, and "critical information systems".

Final Categories (as used in the CIP framework)

From the **Cybersecurity Policy for Critical Infrastructure Protection**:

- **CI sectors**: the policy glossary enumerates CI sectors including **"medical services"** (among other sectors).
- **CI operators**: defined in the policy as "critical social infrastructure providers" (per the Basic Act) and further scoped via **ANNEX 1**.
- **Critical information systems**: information systems required to provide CI services, designated for each CI operator based on degree of impact on CI services.

"Medical services" as a CI sector — what the policy explicitly says

ANNEX 1 (scope/examples) includes:

- **Medical services — Medical facilities (excluding small scale facilities)**, with example critical information systems such as:
    - "medical examination record management systems"
    - "medical examination support systems"
    - "community medical care support systems"

ANNEX 2 (service explanation/outage examples) includes for medical services:

- CI service: "medical examination / examination and treatment"
- Example impacts: hindrance to medical examination support departments; malfunction of medical equipment threatening human life
- Referenced guidance: "Guideline on Safety Management of Medical Information Systems"

Health-sector cybersecurity governance signals from MHLW (evidence from your PDFs)

- **Basic Policy for Cyber-security Measures at Medical Facilities**:
    - The policy context explicitly places healthcare cyber measures alongside:
        * "Basic Act on Cyber-security"

23

- ✳ "Fourth action plan on information security measures for critical infrastructure"
- ✳ and depicts **Healthcare CEPTOAR** within the information-sharing / reporting ecosystem.
  - – It also describes preparation of a **checklist** to facilitate checks at medical facilities and indicates positioning cybersecurity-measure status checks as part of **on-site inspection** framing.

Guidelines on Safety Management of Healthcare Information Systems (Ver. 6.0 outline/major points)

- The version history explicitly notes that **Version 2** was "revised from the viewpoint of healthcare information systems as **critical infrastructure**."
- It also notes that because **online qualification check** became mandatory (from April 2023), "almost all medical facilities, etc., are required to take the network-related security measures" described in the guidelines.

Medical devices cybersecurity (incident handling / reporting) — evidence

From the PMDA/MHLW English reference translation you uploaded (000272598.pdf):

- It describes cybersecurity expectations across the lifecycle (pre-market resilience; post-market vulnerability correction/patching; incident handling) and provides for reporting pathways/forms to PMDA in the described framework.

Grading / Tiering schemes (what we can and cannot claim evidentially)

- **No public numeric thresholding for "medical CI" appears in the CI policy text** (it uses the qualitative boundary "medical facilities (excluding small scale facilities)" in ANNEX 1).
- The CIP framework does define **information-sharing structures and policy measures**, but **a public hospital-tier scoring rubric (A/B/C or Tier 1/2/3)** is **not evidenced** by the sources opened above, so it is **omitted** here.

Health information systems most defensibly "in-scope / critical"

Based strictly on **ANNEX 1 examples for "medical services"** in the CIP policy:

- Medical examination record management systems
- Medical examination support systems
- Community medical care support systems

References (Japan)

1. **Japanese Law Translation (Ministry of Justice). The Basic Act on Cybersecurity (Act No. 104 of 2014).** (link)
2. **Cybersecurity Strategic Headquarters (Japan). The Cybersecurity Policy for Critical Infrastructure Protection** (revised March 8, 2024). (pdf)
3. **National Cybersecurity Office (Japan). Critical Infrastructure Protection Overview.** (pdf)
4. **MHLW (Japan). Basic Policy for Cyber-security Measures at Medical Facilities.** (pdf)
5. **MHLW (Japan). Guidelines on Safety Management of Healthcare Information Systems Ver. 6.0.** (link)
6. **PMDA/MHLW (Japan). Cybersecurity-related medical device safety / reporting material.** (pdf)

CHINA (PEOPLE'S REPUBLIC OF CHINA)

Final categories (what is "highest critical / protected")

1. 关键信息基础设施 **(Critical Information Infrastructure, "CII")** —重点保护 / key protection
   - The Cybersecurity Law provides that the State applies 重点保护 **("key protection")** to CII in listed sectors, **on the basis of the network security graded protection system (网络安全等级保护制度)**, and delegates the **specific scope and protection measures** to the State Council. (CAC)
2. 关键信息基础设施的运营者 **(Operators of CII / "CIIOs")**
   - The Cybersecurity Law contains a dedicated section on **CII operational security** and sets additional obligations for **CII operators** in that section. (CAC)
3. 《关键信息基础设施安全保护条例》 **(State Council Decree No. 745; effective 1 Sept 2021)**
   - These Regulations define CII, establish the supervisory structure, and set out the **industry-regulator "determination / designation" mechanism** (Protection Work Departments drafting designation rules; organizing determinations; notifying operators). (China Law Translate)
4. **Health-sector "highest protected" systems under MLPS (graded protection) — explicit health guidance**
   - The National Health Commission (then Ministry of Health) guidance (2011) states that the **graded protection system has five levels** and lists multiple **health information systems that should be "principally not lower than Level 3."** (National Health Commission)
   - The NHC/NATCM/NCDC measures (2022) state a principle focusing on protection of **CII**, **MLPS Level 3+ networks**, and **important data/personal information** in healthcare institutions. (National Health Commission)

Exact legal / regulatory criteria (what triggers inclusion)

A) The Definition (scope text)

Cybersecurity Law — CII (Article 33 on CAC text)

- CII sectors explicitly listed include: **public communications and information services, energy, transportation, water conservancy, finance, public services, e-government**, and "other" CII whose destruction/loss of function/data leakage may seriously endanger national security / people's livelihood / public interest.
- The provision states this protection is **"on the basis of" the graded protection system**, and that the **specific scope and protection measures are to be formulated by the State Council**. (CAC)

CII Security Protection Regulations (Decree No. 745) — CII definition (Article 2)

- Defines CII by (i) listed sectors (includes **public services, e-government**, etc., and also **national defense technology industry**) and (ii) a harm test (destruction/loss of function/data leakage may seriously endanger national security / people's livelihood / public interest). (China Law Translate)

B) The Thresholds (tests stated in the instruments)

Cybersecurity Law (graded protection baseline)

- The Cybersecurity Law states the State implements the **network security graded protection system** and requires network operators to fulfill specified security protection obligations under that system. (CAC)

Decree No. 745 designation mechanism — criteria for designation rules (Article 9)

- Protection Work Departments must draft **designation rules** and file them with the State Council public security department.
- In drafting designation standards, Article 9 lists three factors:
    1. importance of the network facilities/information systems to core operations in the sector;
    2. degree of harm if destroyed / loses function / data leakage;
    3. impact on other industries/sectors. (China Law Translate)

No numeric thresholds in the designation factors * Article 9 provides factors (importance/harm/impact) and does **not** state numeric thresholds. (China Law Translate)

Grading / tiering scheme

1. **Network security graded protection system (网络安全等级保护制度)**
    - The Cybersecurity Law states that China implements the graded protection system and lists operator obligations under that system. (CAC)
2. **CII protection is explicitly stated as being "on the basis of" graded protection**
    - The Cybersecurity Law provision on CII states 重点保护 for CII **on the basis of** graded protection. (CAC)
3. **Five levels (explicitly stated in the 2011 health-sector guidance)**
    - The 2011 health-sector guidance states: "等级…分为五级" and names each level from Level 1 to Level 5. (National Health Commission)

Incident reporting tests and thresholds

Cybersecurity Law (general incident reporting duty)

- The Cybersecurity Law requires network operators to have incident response plans and to report incidents to competent authorities "according to provisions". (CAC)

Decree No. 745 (Article 18) — CIIO reporting trigger

- CIIOs must report when **major cybersecurity incidents occur** in CII or **major cybersecurity threats are discovered**, to Protection Work Departments and public security organs. (China Law Translate)

Examples of "especially serious" incidents/threats (Decree No. 745, Article 18)

- Article 18 gives examples such as **overall interruption of operations / primary function failures**, **leaks of basic state information and other important data**, **large-scale personal information leaks**, **large economic losses**, or **illegal transmission of a larger scope of information**, triggering onward reporting by Protection Work Departments after receipt. (China Law Translate)

Deadlines

- Article 18 uses "promptly" for onward reporting by Protection Work Departments after receiving a report; no hour/day deadline is specified in the cited Article 18 text. (China Law Translate)

Health-sector clauses / guidance (primary, health-specific)

A) Health systems explicitly "≥ Level 3" in 2011 guidance (NHC/Ministry of Health)

The 2011 guidance states the graded protection system has five levels and then states the following "important health information systems" are **principally not lower than Level 3**:

- **Cross-province national networked systems**:
  - health statistics network direct reporting, infectious disease reporting, health supervision reporting, public health emergency command information systems, etc. (National Health Commission)
- **National/provincial/municipal health information platforms**, and national-level data centers including (examples listed): new rural cooperative medical scheme, health supervision, maternal & child health, etc. (National Health Commission)
- **Core business information systems of Class III Grade A hospitals (三级甲等医院核心业务信息系统).** (National Health Commission)
- **Ministry of Health website system.** (National Health Commission)
- "Other" systems assessed by the technical expert committee as Level 3+. (National Health Commission)

It also states:

- **Annual level evaluation (等级测评)** for Level 3+ health information systems. (National Health Commission)

B) Healthcare institution cybersecurity measures (2022)

The 2022 measures state they are made with reference to multiple laws/regulations including the Cybersecurity Law and the **CII Security Protection Regulations**, and include a principle: * "重点保障关键信息基础设施〖网络安全等级保护第三级及以上网络以及重要数据和个人信息安全" (focus protection on CII, MLPS Level 3+ networks, important data and personal information). (National Health Commission)

Health information systems "most likely" designated

Not determinable from the cited CII national instruments alone. * The CII Security Protection Regulations assign designation to sector Protection Work Departments and require sector designation rules (Articles 9–11). The Regulations do not, in the cited text, list healthcare systems by name as "CII." (China Law Translate)

What is explicitly stated for health (separate from CII designation) * The 2011 and 2022 health-sector instruments explicitly identify multiple health systems as **MLPS Level 3+ targets** and identify protection of **CII** and **MLPS Level 3+ networks** as priorities in healthcare institutions. (National Health Commission)

Public vs confidential

- **Public (instruments):** the Cybersecurity Law text (including the CII chapter) and Decree No. 745 text are publicly available (official Chinese; translations exist). (CAC)
- **Designation outcomes:** Decree No. 745 states operators are **notified** of designation results and that determinations are **reported** to the State Council public security department. (China Law Translate)
- **A public national list of CIIOs is not present in these instruments' text** (i.e., the cited law/regulation text does not contain a list). (CAC)

Latest updates (2025–2026) — primary confirmation

- Xinhua reports the NPCSC passed the decision amending the Cybersecurity Law on **28 Oct 2025** and that it **takes effect 1 Jan 2026**. (Xinhua News)
- The CAC page for the Cybersecurity Law states the law is **revised according to the 2025-10-28 NPCSC decision** (as shown in the header). (CAC)

References (China)

1. **Cyberspace Administration of China (CAC)** — "中华人民共和国网络安全法" (official Chinese text; header shows 2025 revision basis; includes CII chapter). (CAC)
2. **China Law Translate** — "Regulations on Critical Information Infrastructure Security Protections" (State Council Decree No. 745) (translation; Articles 2, 9–11, 18 etc used). (China Law Translate)
3. **National Health Commission (NHC)** — 2011 "卫生行业信息安全等级保护工作的指导意见" (卫办发〔2011〕85号) (five levels; ≥ Level 3 system list; annual evaluation). (National Health Commission)
4. **NHC / NATCM / NCDC** — 2022 "医疗卫生机构网络安全管理办法" (国卫规划发〔2022〕29号) (focus on CII and MLPS Level 3+ networks, etc.). (National Health Commission)
5. **Xinhua (新华网)** — report that amendments were passed 2025-10-28 and effective 2026-01-01. (Xinhua News)
6. **English.gov.cn** — State Council release summarizing Decree No. 745 effective date (Sept 1, 2021). (State Council of China)

SOUTH KOREA

Final categories

Act on the Protection of Information and Communications Infrastructure (정보통신기반 보호법) establishes a **designation-based "critical infrastructure" regime** for **information and communications infrastructure**:

1. **Information and Communications Infrastructure** (정보통신기반) — defined term. (E-Law)
2. **Critical Information and Communications Infrastructure** (주요정보통신기반시설) — **information and communications infrastructure designated** as "critical" by the head of a central administrative agency (or, for certain local-government-supervised organizations, by the competent Minister in consultation). (E-Law)
3. **Management Organization** — an organization that manages critical information and communications infrastructure, with statutory duties to formulate and implement protection measures and related submissions/roles. (E-Law)

The **Enforcement Decree** prescribes **procedures and required contents** for designation, publication/notification, vulnerability analysis timing, protection-measures submission, and incident notification contents. (E-Law)

Exact legal / regulatory criteria (primary texts)

A) What may be designated as "critical"

A central administrative agency head may designate infrastructure under their jurisdiction as **critical information and communications infrastructure** by taking into account the **five factors** below:

1. national/social importance of duties performed by the managing organization
2. dependence of those duties on the infrastructure
3. inter-connection with other infrastructure
4. areas/extent of damage to national security, economy, society if an intrusion incident occurs
5. probability of intrusion incidents and ease of restoration (E-Law)

Additional legal points in the Act on designation:

- The agency head **may request data** necessary to decide designation. (E-Law)
- The agency head **may revoke** designation when the relevant affairs are abolished/suspended/changed. (E-Law)
- The agency head must **submit designation/revocation for deliberation** by the Committee (with authority for the Committee to hear opinions). (E-Law)
- The agency head must **publicly announce** designation/revocation **unless** the Committee deliberates that non-announcement is necessary for national security. (E-Law)

B) Decree: how "designation" is operationalized

The Decree specifies a stepwise process around a **"designation unit"** and evaluation:

- **Selection of designation units** (Decree Art. 13): central administrative agency head requires the organization to select a "designation unit," and may examine/adjust reasonableness. (E-Law)
- **Self-evaluation for designation** (Decree Art. 14): agency head may issue evaluation guidelines; organization evaluates and submits results. (E-Law)
- **Review of evaluation** (Decree Art. 15): agency head reviews whether self-evaluation is objective/appropriate with reference to Act Art. 8(1) factors; may require re-evaluation in specified circumstances. (E-Law)
- **Recommended designation decision timeline** (Decree Art. 16-2(3)): where designation is recommended under Act Art. 8-2(1), the agency head must decide whether to designate after designation-unit selection, self-evaluation, and review **within 60 days**. (E-Law)

C) Public notice / publication requirements (Act + Decree)

- Act: designation/revocation must be **publicly announced**, with a national-security exception after Committee deliberation. (E-Law)
- Decree Art. 16: when designating or revoking designation, the agency head must notify the management organization "without delay" and publish specific fields in the **Official Gazette**:
    1. designation number
    2. name of critical information and communications infrastructure
    3. name of management organization
    4. performing duties
    5. grounds for designation/revocation (E-Law)

Obligations tied to "critical" designation (Act + Decree)

A) Protection measures and submission

- Act Art. 5(1): management organization must formulate and implement **physical and technological** protection measures, linked to vulnerability analysis results. (E-Law)
- Act Art. 5(2): management organization submits details of measures to the competent central administrative agency (with stated exception). (E-Law)
- Decree Art. 8: measures for the following year must be submitted **by every August 31**. (E-Law)

B) Vulnerability analysis and timing

- Act Art. 9(1): management organization analyzes and evaluates vulnerabilities "on a regular basis as prescribed by Presidential Decree." (E-Law)
- Decree Art. 17(1)–(3):
    – first analysis within **6 months** of designation (extendable to **9 months** with approval, per stated condition)
    – thereafter **each year** (with an exception allowing earlier analysis if serious changes occur or deemed necessary)
    – if ordered under Act Art. 9(2), analysis within **6 months** of receiving the order (E-Law)

C) Roles (CISO concept)

- Act Art. 5(4): management organization designates a **chief information security officer** (with stated exception). (E-Law)
- Decree Art. 9: specifies who may be designated and enumerates supervisory responsibilities (including measures, technical support requests, vulnerability analysis, compliance with guideline/measure orders, incident notification, and recovery measures). (E-Law)

D) Protection guidelines

- Act Art. 10: central administrative agencies may establish protection guidelines and recommend management organizations follow them; guidelines must be revised/supplemented regularly considering technological advancements. (E-Law)
- Decree Art. 20(1)–(2): protection guidelines include (i) management/operation of an information protection system, (ii) vulnerability analysis & incident prevention, (iii) incident response & recovery; and must be notified to management organizations when formulated/revised/supplemented. (E-Law)

E) Cyber security incident notification content (Decree)

- Decree Art. 21(1): notification includes (1) date/time and facility, (2) details of damage, (3) other matters necessary for swift response and recovery. (E-Law)

Grading / tiering scheme

In the Act + Enforcement Decree texts cited above, **designation is a binary status** (designated or not designated as "critical information and communications infrastructure"); **no numeric or multi-tier classification scale** appears in these provisions. (E-Law)

What is public vs confidential

- **Public:** the Act requires public announcement of designation/revocation (subject to the national-security exception). (E-Law)
- **Public:** the Decree requires Official Gazette publication of specific designation fields. (E-Law)
- **May be withheld (national security):** the Act permits non-public announcement after Committee deliberation when necessary for guaranteeing national security. (E-Law)

References (South Korea)

1. **Korea Legislation Research Institute (KLRI). Act on the Protection of Information and Communications Infrastructure** (English translation page; includes Arts. 2, 5–13, etc.). (E-Law)
2. **Korea Legislation Research Institute (KLRI). Enforcement Decree of the Act on the Protection of Information and Communications Infrastructure** (English translation page; includes Arts. 8–9, 13–18, 20–22, etc.). (E-Law)

3. **Korea Law Information Center (law.go.kr). Act on the Protection of Information and Communications Infrastructure** (English statute page). ([Korea Law Information Center](#))

FRANCE

Translation note: English translations below are **unofficial** glosses of the cited French legal terms/phrases, provided for readability. All legal terms remain as defined in the cited French primary texts.

Final categories (what is "highest critical / protected")

1. **Opérateur d'importance vitale (OIV)** — *(English: "Operator of Vital Importance")* — category defined in **Code de la défense, Article R.1332-1**.
2. **Secteur d'activités d'importance vitale (SAIV)** — *(English: "Sector of Vital-Importance Activities")* — criteria in **Code de la défense, Article R.1332-2**; SAIV list fixed by **Arrêté du 2 juin 2006 modifié**.
3. **Systèmes d'information d'importance vitale (SIIV)** — *(English: "Vital-Importance Information Systems")* — definition + secrecy of the SIIV list in **Code de la défense, Article R.1332-41-2**.
4. **Health SAIV sub-sectors with SIIV rules + incident modalities fixed by ministerial orders** (examples from 17 April 2023 JORF texts):
   - « **Établissements de santé** » — *(English: "Health establishments / healthcare facilities")* (Arrêté du 17 avril 2023).
   - « **Veille et alerte sanitaires** » — *(English: "Health surveillance and health alerts")* (Arrêté du 17 avril 2023).

Exact legal / regulatory criteria (what triggers inclusion)

A) The Definition

A1. OIV (operator-level designation test) — Code de la défense, Article R.1332-1 (II)

Key French legal phrases → English gloss:

- « **obérer gravement** » → "seriously impair / severely undermine"
- « **mettre gravement en cause la santé ou la vie de la population** » → "seriously jeopardise the health or life of the population"
- « **malveillance, sabotage, terrorisme** » → "malicious acts, sabotage, terrorism"

A2. SAIV (sector-level criteria) — Code de la défense, Article R.1332-2

Key French legal phrases → English gloss:

- « **besoins essentiels pour la vie des populations** » → "essential needs for the life of the population(s)"
- « **difficilement substituables ou remplaçables** » → "difficult to substitute or replace"
- « **danger grave pour la population** » → "serious danger for the population"

A3. SIIV (system-level definition) — Code de la défense, Article R.1332-41-2

Key French legal phrase → English gloss:

- « **couverte par le secret de la défense nationale** » → "covered by national defence secrecy"

B) The Thresholds

B1. OIV impact threshold language (qualitative test) — uses the French qualitative terms above (e.g., « **obérer gravement** », « **mettre gravement en cause…** »). **B2. SAIV substitutability + serious danger tests (qualitative tests)** — uses « **difficilement substituables ou remplaçables** » and « **danger grave pour la population** ».

Grading / tiering scheme

- **Binary designation**: designated **OIV** vs non-designated.
- **OIV designation orders**: « **ne sont pas publiés** » → "are not published"; and **not communicable** under the cited CRPA provisions.
- **No public tiering scheme stated** in the cited SAIV/OIV/SIIV provisions.

Incident reporting tests and thresholds

General SIIV incident-information rule (no hour-based deadline stated here) — **Code de la défense, Article R.1332-41-10**

Key French legal phrases → English gloss:

- « **dès qu'ils ont connaissance** » → "as soon as they become aware"
- « **au fur et à mesure de l'avancement de l'analyse** » → "as the analysis progresses"
- **(Arrêté not published)** « **n'est pas publié** » / **notification to persons with a need to know** → "not published / notified to persons who need to know"

Health sub-sector orders (examples) — incident types specified by annexes (not published)

Key French legal phrase → English gloss:

- « **ne sont pas publiées** » (Annexes II–IV) → "are not published"

Health information systems "most likely" designated

- **OIV designation list**: designation orders **not published** (« **ne sont pas publiés** ») and **not communicable**.
- **SIIV lists**: covered by **national defence secrecy** (« **secret de la défense nationale** »).
- **Health-related SAIV sub-sectors explicitly named** in cited JORF texts:
    - « **Établissements de santé** » *("Health establishments / healthcare facilities")*
    - « **Veille et alerte sanitaires** » *("Health surveillance and health alerts")*

Public vs Confidential

Public

- Definitions and criteria in the **Code de la défense** (OIV/SAIV/SIIV; incident information rule).
- SAIV list in **Arrêté du 2 juin 2006 modifié**, including « **Santé** » *("Health")*.
- Health sub-sector orders stating annex publication status and rule structure.

Confidential / not published

- **OIV designation orders**: **not published** / not communicable.
- **SIIV lists**: covered by **national defence secrecy**.
- **Annexes II–IV** of cited 17 April 2023 health sub-sector orders: **not published**.

Latest updates (2025–2026)

- **EU NIS2 transposition status (France)** — Commission status page entries (dates shown on the cited page).
- **Assemblée nationale dossier** — bill docket entries (dates shown on the cited page).

References (France)

1. **Code de la défense — Article R.1332-1** (OIV criteria). (Legifrance)
2. **Code de la défense — Article R.1332-2** (SAIV criteria). (Legifrance)
3. **Code de la défense — Article R.1332-3** (OIV designation secrecy). (Legifrance)
4. **Arrêté du 2 juin 2006** (SAIV list includes « Santé »). (Legifrance)
5. **Code de la défense — Article R.1332-41-2** (SIIV definition). (Legifrance)
6. **Code de la défense — Article R.1332-41-10** (Incident notification). (Legifrance)
7. **Arrêté du 17 avril 2023 — « Établissements de santé »**. (Legifrance)
8. **Arrêté du 17 avril 2023 — « Veille et alerte sanitaires »**. (Legifrance)
9. **Assemblée nationale — Dossier législatif (Cybersécurité)**. (Link)
10. **European Commission — NIS2 Implementation (France)**. (Link)

NORWAY

Note: Norway's core legal framework for digital security is the **Digital Security Act (digitalsikkerhetsloven)**, with implementing **Digital Security Regulations** that entered into force **1 October 2025**.

Final Categories

1) Providers of socially important services (tilbydere av samfunnsviktige tjenester)

- The Act applies to **providers of socially important services** under § 6 **in the sectors**: energy, transport, **health**, water supply, bank, financial market infrastructure, and digital infrastructure.

2) Providers of digital services (tilbydere av digitale tjenester)

- The Act applies to **providers of digital services** under § 9.
- § 9 lists: **online marketplace**, **online search engine**, and **cloud computing service**.

3) Health sector code of conduct (sector guidance)

- **Code of Conduct for Information Security and Data Protection in the Health Care Sector (Version 7.0)** (the "Code"), including stated version metadata and applicability date.

Exact Legal / Regulatory Criteria (primary texts)

A) Statutory scope (Digital Security Act)

Scope: sectors include health

- The Act applies to providers of socially important services under § 6 in the sectors including **health**.

Entry into force

- § 20 states the Act enters into force at the time determined by the King; the Lovdata rendering notes "From 1 Oct 2025 …".

B) "Provider of a socially important service" — § 6 (Act)

A provider under § 6 is an entity that: * **delivers a service** in one of the listed sectors (including **health**), **and** * is **dependent on network and information systems** to deliver that service, **and** * the service is **important for maintaining fundamental societal functions or people's basic needs**, and an incident would have **significantly disruptive impact** on delivery of the service.

C) Security requirements for providers of socially important services — § 7 (Act)

§ 7 requires **appropriate and proportionate technical and organisational measures** and lists specific risk/assurance aims, including: preventing incidents and limiting consequences; ensuring a level of security appropriate to risk; and maintaining continuity/availability elements as described in the provision (items (a)–(g)).

D) Incident notification duty for providers of socially important services — § 8 (Act) + reporting timelines (Regulations)

Duty to notify (Act § 8)

- Providers must **notify** the supervisory authority **without undue delay** about incidents with **significant impact** on continuity of the service.
- The Act lists factors for assessing whether impact is "significant" (users affected, duration, geographic area, extent of functionality failure, and impact on economic and societal activity).

Reporting steps and timelines (Regulations § 20)

The Regulations specify a staged reporting sequence for incidents with significant impact:

- **Early warning**: "as soon as possible and no later than **24 hours** after the provider becomes aware …".
- **Notification**: "as soon as possible and no later than **72 hours** after the provider becomes aware …".
- **Final report**: "no later than **one month** after submission of the notification …".

E) Providers of digital services — § 9, § 10, § 11 (Act)

Category definition (Act § 9)

- § 9 lists the digital services: **online marketplace**, **online search engine**, **cloud computing service**.

Security requirement (Act § 10)

- Providers of digital services must implement **appropriate and proportionate technical and organisational measures** and lists areas to address (security of systems and facilities, incident handling, business continuity management, monitoring/auditing/testing, compliance with standards, etc.).

Incident notification duty (Act § 11)

- Providers of digital services must **notify** the supervisory authority **without undue delay** about incidents with **substantial impact** on provision of the service, and the section lists assessment factors (users affected, duration, geographic spread, extent of disruption, impact on economic and societal activities).

F) Supervisory and enforcement elements (Act + Regulations)

Supervisory authority appointment (Act § 13)

- "The King appoints one or more supervisory authorities …".

Information access / inspections (Act § 14)

- Providers must provide information required by the supervisory authority and provide access to premises and equipment; this applies "without hindrance of statutory confidentiality".

Administrative reactions (Act §§ 15–17)

- § 15: corrective orders ("pålegg om retting") with deadline.
- § 16: coercive fine ("tvangsmulkt").
- § 17: violation fine ("overtredelsesgebyr") for intentional/negligent breaches of §§ 7, 8, 10, 11 or 14.

Maximum violation fine level (Regulations § 24)

- Regulations § 24 describes violation fine upper limits and states: "In any case, the fine … may not exceed **NOK 50 million**."

Designation / listing mechanisms (Regulations § 1 — sector enumerations)

The Regulations define "providers of essential services" (providers of socially important services) and list multiple categories. For the **health** sector, the list includes:

- **Regional health enterprises** (regional helseforetak) and the **Norwegian Health Network** (Norsk Helsenett SF).
- Providers responsible for **pre-hospital emergency medical services** under the Health and Care Services Act § 3-2(1) and the Municipal Health and Care Services Act § 3-2a.
- Providers responsible for **specialist medical emergency response services** under the Specialist Health Services Act § 2-2.

Health-specific clauses / guidance covered (only what the PDFs state)

1) Health sector is explicitly in the Act's sector scope

- "Health" is explicitly listed among the sectors for providers under § 6.

2) Health sector provider types are explicitly listed in the Regulations

- The Regulations enumerate specific health-sector organisations/services as providers of essential services (examples listed above).

3) Health Care Sector Code of Conduct (Version 7.0) — what the Code states

Version metadata / applicability

- The Code document states "Version 7.0" and "Applicable from 01/10/2025" (and includes approval/publishing metadata in the same section).

Scope statement: "Who does the Code apply to" (section 1.3)

- The Code includes a dedicated section "1.3 Who does the Code apply to" describing the health and care sector scope in the document itself.

Relationship to legislation (section 1.4)

- The Code includes a section "1.4 Relationship between the Code and applicable legislation" that describes how the Code relates to legal requirements.

Minimum requirement themes (section 3.2)

- The Code includes section "3.2 Minimum requirements for information security and data protection" that enumerates minimum requirements (including core security properties and related operational expectations) in the text.

References (Norway)

1. **Stortinget / Lovdata.** *Lov om digital sikkerhet (digitalsikkerhetsloven)* (2023-12-20-108). (Lovdata)
2. **Lovdata.** *Forskrift om digital sikkerhet (digitalsikkerhetsforskriften)* (FOR-2025-06-20-1131). (Lovdata)
3. **Norwegian Directorate of Health (Helsedirektoratet).** *Code of Conduct for Information Security and Data Protection in the Health Care Sector (Normen) — Version 7.0.* (Link)

SWITZERLAND

Final categories (what is "highest critical / protected")

- **Betreiberinnen von kritischen Infrastrukturen** (operators of critical infrastructures) subject to the **Pflicht zur Meldung von Cyberangriffen** (duty to report cyberattacks). **Primary basis:** *Informationssicherheitsgesetz (ISG)*, **Art. 74a–74i**. ([Newsd](#))
- **Meldepflicht (cyberattack reporting duty) implementing ordinance**. **Primary basis:** *Cybersicherheitsverordnung (CSV)* (ordinance), incl. **Art. 12–19**.

Exact legal / regulatory criteria (what triggers inclusion)

Subsection A (The Definition): the specific text defining the scope

Scope by category (ISG Art. 74b "Bereiche – Die Meldepflicht gilt für") includes, among other sectors, the following health-relevant categories:

- **"Spitäler, die auf der kantonalen Spitalliste … aufgeführt sind"** (hospitals listed on a canton's hospital list). ([Newsd](#))
- **"medizinische Laboratorien mit einer Bewilligung … des Epidemiengesetzes"** (medical laboratories with a permit under the Epidemics Act). ([Newsd](#))
- **"Unternehmen … [mit Bewilligung] … von Arzneimitteln … oder Medizinprodukte … herstellen oder vertreiben"** (companies authorised for medicines, and companies that manufacture or distribute medical devices as specified). ([Newsd](#))

Exclusion mechanism (ISG Art. 74c): the Federal Council must exclude categories where cyberattack-caused outages/malfunctions are **unlikely** (e.g., low IT dependence) or would have **only minor impacts** (e.g., few persons affected; absorbed by other critical infrastructures; low macroeconomic loss potential). ([Newsd](#))

Ordinance-level exclusions (CSV Art. 12):

- CSV specifies sectoral exclusion conditions for listed categories (e.g., higher education; energy; transport; post; civil aviation etc.).

Subsection B (The Thresholds): quantitative or qualitative tests

Reportable cyberattack conditions (ISG Art. 74d): a cyberattack on a critical infrastructure must be reported if there are indications that:

- **functionality is endangered** (of the affected CI or another CI), or

- **a foreign state** executed/caused it, or

- it **led to or could lead to manipulation / outflow of information**, or

- it remained **undetected for more than 30 days**;

and it **must always** be reported if linked to **extortion, threat, or coercion** against the operator or its employees. (Newsd) **Ordinance definitions used for applying these tests (CSV Art. 14):**

- Functionality "endangered" if **employees/third parties are affected by system interruptions** or operations can be maintained **only using emergency plans**.

- "Manipulation / outflow" exists if **business-relevant information** is viewed/changed/disclosed by unauthorized persons, or a **data security breach notification under DSG Art. 24** has been made.

- "Undetected for a longer period" is defined as **more than 90 days** since the incident.

- "Extortion/threat/coercion" link is defined by CSV.

Grading / tiering scheme

- **Binary scheme (in-scope vs out-of-scope)**: the reporting duty applies if the entity falls within **ISG Art. 74b** and is not excluded under **ISG Art. 74c / CSV Art. 12**. (Newsd)

Incident reporting tests and thresholds

Deadlines (primary text):

- **24-hour reporting period:** CSV refers to a **"Meldefrist von 24 Stunden nach der Entdeckung des Cyberangriffs"** (reporting period of 24 hours after discovery).
- **Completion window (if information is missing):** if not all required information is known within the 24-hour period, BACS grants **14 days** to supplement the report.

Triggers (primary text):

- **ISG Art. 74d** conditions (functionality endangered; foreign state; manipulation/outflow; undetected >30 days; always if extortion/threat/coercion). (Newsd)
- **CSV Art. 14** definitions for applying "functionality endangered", "manipulation/outflow", "undetected", and "extortion/threat/coercion".

Health information systems "most likely" designated

Explicit in law

- The primary instruments define **entity categories** (e.g., hospitals on cantonal hospital lists; permitted medical laboratories; authorised medicines/medical-device businesses). They do **not** list specific health **information system types** (e.g., EHR, PACS) as named items. (Newsd)

Public vs Confidential

- **Public:** ISG and CSV texts (scope categories; exclusions; reportable-incident tests; deadlines; ordinance entry-into-force). (Newsd)

- **Confidential / not in these primary texts:** no consolidated list of specific obligated entities is provided in ISG/CSV; certain categories reference external legal lists/permits (e.g., "kantonale Spitalliste"; Epidemics Act permits). (Newsd)

Latest updates (2025–2026)

- **CSV entry into force:** "Diese Verordnung tritt am **1. April 2025** in Kraft." (CSV Art. 19).
- **No additional 2025–2026 amendments** are stated in the accessed primary texts beyond the above entry-into-force provision.

References (Switzerland)

1. **Federal Council (Bund).** *Informationssicherheitsgesetz (ISG)*. (pdf)
2. **Federal Council (Bund).** *Cybersicherheitsverordnung (CSV)*. (Fedlex)

TAIWAN

Final categories (what is "highest critical / protected")

1. **Critical infrastructure providers**

   Primary basis: Cyber Security Management Act (CSMA) — Chapter III, **Article 20** (designation + obligations for "critical infrastructure providers"). (Law Moda)

2. **Specific non-government agencies** (regulated non-government entities, including CI providers and others covered by the Act)

   Primary basis: CSMA — Chapter III (e.g., **Articles 21–24** set obligations for "specific non-government agencies," including incident notification/reporting mechanisms). (Law Moda)

3. **Critical Information Infrastructure (CII)** (defined within Taiwan's national CI protection guidance)

   Primary basis: Executive Yuan Office of Homeland Security (OHS) — *Guidelines for National Critical Infrastructure Protection* (definition of **CII** as systems/SCADA supporting continuous operation of national critical infrastructures).

Exact legal / regulatory criteria (what triggers inclusion)

A) The Definition (scope text)

- **National Critical Infrastructure (CI)** definition (OHS Guidelines): assets/systems/networks (public/private; physical/virtual) whose disruption may negatively impact government/society, cause casualties, losses, economic downturn, environmental changes, or damage national security/interests.
- **Critical Information Infrastructure (CII)** definition (OHS Guidelines): "vital information and communication systems or SCADA" dealing with core task functions and supporting continuous operation of national CI; managed under a single authority according to the CI sector it belongs to.
- **Critical infrastructure providers** designation construct (CSMA Article 20): the central competent authority for the relevant sector **designates critical infrastructure providers**, submits the designation **for approval by the Executive Yuan**, and notifies approved entities in writing. (Law Moda)

B) The Thresholds (quantitative / qualitative tests)

- **No numeric thresholds are stated** in the cited legal text for when an entity becomes a "critical infrastructure provider." The designation mechanism is described as an administrative designation/approval process (CSMA Article 20). (Law Moda)

Grading / tiering scheme

- **Cyber security responsibility levels (A–E)** (classified **from high to low**): **Level-A, Level-B, Level-C, Level-D, Level-E**.

  Primary basis: *Regulations on Classification of Cyber Security Responsibility Levels*, **Article 2** (as published in MODA's CSMA-related regulations compilation). ([Ministry of Digital Affairs](#))

- **Incident severity levels (Level-1 to Level-4)** used for response requirements:

  The *Regulations on the Notification and Response of Cyber Security Incident* define **level-1, level-2, level-3, level-4** cyber security incidents (including distinctions involving **core business information**, **core information and communication systems**, scope of service interruption, and geographic/scale impact). ([Ministry of Digital Affairs](#))

Incident reporting tests and thresholds

Deadlines

From the *Regulations on the Notification and Response of Cyber Security Incident*:

- **Government agencies**:
    - Must **complete verification** within **8 hours** for **level-1/2** incidents and within **2 hours** for **level-3/4** incidents (Article 5). ([Ministry of Digital Affairs](#))
    - Must **complete damage control or recovery** within **72 hours** for **level-1/2** and within **36 hours** for **level-3/4** (Article 6). ([Ministry of Digital Affairs](#))
- **Specific non-government agencies** (including those designated):
    - When aware of a cyber security incident, must **notify** the central competent authority for the relevant sector; for **level-3/4**, notification must be **within 1 hour** (Regulations, Article 11). ([Ministry of Digital Affairs](#))
    - After completing damage control or recovery, must submit an **investigation/handling report**, and then submit a **corrective action report** (Articles 11–12). ([Ministry of Digital Affairs](#))

Triggers (what counts as reportable)

- The same regulation defines incident **levels 1–4**; the level definitions reference (among other factors) whether the event affects **core business information** and/or a **core information and communication system**, and the scope/duration/extent of disruption (Article 2). ([Ministry of Digital Affairs](#))

Health information systems "most likely" designated

- **Not stated in cited primary texts.**

  The OHS Guidelines classify national CI into **eight sectors**, one of which is **"emergency rescue and hospitals"**. The Guidelines also define **CII** as the vital ICT/SCADA supporting continuous CI operations. However, the cited sources do **not** publish a system-by-system list for healthcare.

Public vs Confidential

Public (in cited sources):

- CSMA (legal obligations and the designation mechanism for "critical infrastructure providers," incident notification duty, etc.). (Law Moda)
- OHS Guidelines (definitions of CI/CII; sector classification including hospitals).

Confidential (not evidenced here):

- **Not stated in cited primary texts** whether the specific lists of designated providers/assets are public or confidential.
- The OHS Guidelines' table of contents includes a section titled **"Classified and sensitive information/Confidentiality requirement"** (Chapter 4, Section 1), but this chapter does not claim what specific lists are or are not disclosed beyond what is explicitly shown.

Latest updates (2025–2026)

Cyber Security Management Act revised and promulgated:

- Taiwan's official MODA law database shows the CSMA **"Date: 2025.09.24"** and notes it was **"Revised and promulgated a total of 35 articles… on September 24, 2025,"** with **"date of enforcement… determined by the Executive Yuan."** (Law Moda)

Competent authority (as reflected in the revised CSMA text):

- The same official text states **"The competent authority… is the Ministry of Digital Affairs"** (Article 2). (Law Moda)

References (Taiwan)

1. **Ministry of Digital Affairs (MODA). Cyber Security Management Act** (English law database; revision dated 2025-09-24). (Law Moda)
2. **Ministry of Digital Affairs (MODA). Consolidated PDF of CSMA + related regulations**. (Ministry of Digital Affairs)
3. **Executive Yuan Office of Homeland Security. Guidelines for National Critical Infrastructure Protection** (2018 revision).
4. **MODA / Administration for Cyber Security. Critical Infrastructure Protection (CIIP) overview**. (Ministry of Digital Affairs)

THAILAND

Final categories (what is "highest critical / protected")

- **"Critical Information Infrastructure" (CII)** — defined term in the **Cybersecurity Act, B.E. 2562 (2019)** (unofficial English translation in Government Gazette format).
- **"Organization of Critical Information Infrastructure" (CII Organization)** — defined term in the **Cybersecurity Act, B.E. 2562 (2019)**.
- **Cyber Threat levels** — **non-critical / critical / crisis** levels defined in the **Cybersecurity Act, B.E. 2562 (2019)**.

Exact legal / regulatory criteria (what triggers inclusion)

Subsection A (The Definition): the specific text defining the scope

- **"Critical Information Infrastructure"**: "the computer or computer system" used by a Government Agency or private organization in operations relating to **maintaining national security, public security, national economic security, or infrastructures in the public interest**.
- **"Organization of Critical Information Infrastructure"**: a Government Agency or private organization that **has a mission of or provides a CII service**.
- **Committee designation power (Section 49):** the Committee prescribes (by notification) characteristics of organizations with missions/services in specified aspects, including **"public health"**.

Subsection B (The Thresholds): quantitative or qualitative tests

- **Aspect-based trigger (qualitative):** Section 49 lists aspects for which organizations may be prescribed as CII Organizations; **"public health"** is one listed aspect.
- **Case-by-case review (qualitative):** Section 49 states the Committee "shall consider and review… on a case-by-case basis."
- **No numeric outage/time thresholds** for CII designation appear in the provided Act text.

Grading / tiering scheme

- **Three-level Cyber Threat classification (Section 60): non-critical level / critical level / crisis level**.
- **Public health referenced in threat effects (Section 60(2)):** "critical level" includes effects on "…economy, **public health**, public safety, or the public order…" such that the CII operation could not operate or provide service.

Incident reporting tests and thresholds

Deadlines

- **Section 57 (CII incident reporting):** where a Cyber Threat is "significantly occurring" to a CII Organization's system, it "shall report" to the Office and the Supervising/Regulating Organization; the CRC "may prescribe criteria and method" of reporting. **No fixed hour/day deadline is stated in Section 57 in the provided Act text.**
- **Section 58 ("without delay"):** if examination shows there is or may be a Cyber Threat to an information system under a Government Agency or CII Organization, the organization shall notify the Office and its Supervising/Regulating Organization **"without delay."**
- **Section 54 (annual assessment + 30-day submission):** a CII Organization must conduct risk assessment / cybersecurity examination **at least once per year** and submit a summary report to the Office **within 30 days** after completion.

Triggers (what counts as a reportable incident)

- **Section 57 trigger:** "Cyber Threat significantly occurring" to the system of a CII Organization.
- **Section 58 trigger:** examination results show there "is or may be" a Cyber Threat to the relevant information system.
- **Penalty for non-reporting (Section 73):** failure by a CII Organization to report a Cyber Threat incident under Section 57 (without reasonable cause) — **fine not exceeding Baht 200,000**.

Health information systems "most likely" designated

- **Explicit in the provided primary text:** Section 49 includes **"public health"** as an aspect for which the Committee may prescribe organizations as CII Organizations.
- **Not specified in the provided primary text:** the Cybersecurity Act text provided does **not** enumerate specific **health information system types** (e.g., EHR, LIS, radiology PACS) as CII, and does **not** provide a published list of designated health entities within the provided documents.
- **Process stated in the Act:** designation occurs via **Committee notification** prescribing characteristics of organizations in the listed aspects (including public health), with consideration rules published in the Government Gazette and case-by-case review.

Public vs Confidential

Public (in provided primary text)

- The Act states that Committee rules for consideration under Section 49 "shall be published in the Government Gazette."

Confidentiality obligations in provided health-sector primary text (separate statute):

- **National Health Act, B.E. 2550 (2007), Section 7:** "Personal health information shall be kept confidential," and disclosure is restricted except by the person's will or where required

by specific law.

Latest updates (2025–2026)

CII List Revision (September 2025):

- On 16 September 2025, the NCSC published a notification in the Royal Gazette revising the official list of Critical Information Infrastructure (CII) organizations, specifically covering seven key sectors including **public health**. This update modernizes the 2023 classifications and clarifies regulatory oversight for both public and private essential service providers.

Website Security Standard (September 2025):

- A new Website Security Standard was issued on 16 September 2025 under the Cybersecurity Act, establishing mandatory technical protocols (encryption, incident management, etc.) for CII operators and government agencies.

References (Thailand)

1. **Office of the National Cyber Security Committee (NCSC). Cybersecurity Act, B.E. 2562 (2019)**. (link)
2. **National Health Commission Office. National Health Act, B.E. 2550 (2007)**. (link)
3. **Royal Thai Government Gazette. NCSC Notification Re: List of Critical Information Infrastructure Organizations (2025)**. (link)
4. **NCSC Thailand. Notification Re: Website Security Standard for Government and CII Organizations (2025)**.

HONG KONG (HKSAR)

Final Categories

Protection of Critical Infrastructures (Computer Systems) Ordinance (Ord. No. 4 of 2025; Cap. 653) creates the following legal categories:

1. **Critical infrastructure** (definition linked to **Schedule 1 sectors**, including **Healthcare services**) (Legislative Council of Hong Kong)
2. **Specified critical infrastructure** (a "critical infrastructure" that is **specified for** a particular **regulating authority**) (Legislative Council of Hong Kong)
3. **Regulating authorities**
   - **Commissioner of Critical Infrastructure (Computer-system Security)** (as regulating authority) (Legislative Council of Hong Kong)
   - **Designated authorities** in **Schedule 2** (Monetary Authority; Communications Authority) (Legislative Council of Hong Kong)
4. **CI operator** (organization **designated** under section 12) (Legislative Council of Hong Kong)
5. **Critical computer system** (computer system **designated** under section 13) (Legislative Council of Hong Kong)
6. **Category 1 / Category 2 / Category 3 obligations** (defined by reference to **Part 4** divisions) (Legislative Council of Hong Kong)

Commencement: a Government notice states the Ordinance **comes into operation on 1 January 2026** (with commencement notice published in the Gazette on 27 June 2025). (Communications Authority)

Exact Legal / Regulatory Criteria (primary text)

A) "Critical infrastructure" — definition + sectors

Definition (section 2): "critical infrastructure" means an infrastructure that is:

- **related to a sector specified in Schedule 1**, and
- **provides an essential service in Hong Kong**, and
- the disruption/compromise described in the definition would **hinder or substantially affect** maintenance of **critical societal and economic activities in Hong Kong**. (Legislative Council of Hong Kong)

Schedule 1 sectors (for the definition of "critical infrastructure") include: **Energy; Information technology; Banking and financial services; Air transport; Land transport; Maritime transport; Healthcare services; Telecommunications and broadcasting services**. (Legislative Council of Hong Kong)

B) "Specified critical infrastructure" — which regulator applies

For a **critical infrastructure** to be a **specified critical infrastructure** (section 2(3)):

- it must be **related to** a sector in **Schedule 1**, and
- it is specified **for a designated authority** if it is related to a sector in **Schedule 2** and is operated by a **regulated organization** in Schedule 2; otherwise it is specified **for the Commissioner**. (Legislative Council of Hong Kong)

Designated authorities in Schedule 2:

- **Monetary Authority** (for **Banking and financial services**)
- **Communications Authority** (for **Telecommunications and broadcasting services**) (Legislative Council of Hong Kong)

Regulating authority rule (section 5): the **Commissioner** is the regulating authority for CI operators **unless** the operator operates a specified critical infrastructure specified for a **designated authority**, in which case the **designated authority** regulates that operator. (Legislative Council of Hong Kong)

C) CI operator — designation test (section 12)

A regulating authority may **designate an organization** as a **CI operator** if the authority determines the organization has **ownership or control** in relation to the **operation** of the whole or part of a specified critical infrastructure, including (examples listed in section 12(2)):

- ownership/control of the whole/part of the infrastructure;
- operation of the whole/part;
- ability to **direct or influence** the operation. (Legislative Council of Hong Kong)

In deciding whether to designate, section 12(3) lists factors including:

- **degree of ownership or control** in relation to operation;
- whether the organization can **direct or influence** the operation;
- any other factor the authority considers relevant. (Legislative Council of Hong Kong)

D) Critical computer system — designation test (section 13)

A regulating authority may **designate a computer system** as a **critical computer system** of a specified critical infrastructure if (section 13(1)):

- it is a computer system **operated by** the CI operator or another person;
- it is **accessible by the CI operator in or from Hong Kong**; and
- it is **essential to the core function** of the infrastructure. (Legislative Council of Hong Kong)

In designating, section 13(2) lists factors including:

- extent to which the system is essential to the core function;
- whether it can be substituted;
- effect of compromise on operation/provision of essential service;
- connectivity/exposure;
- other factor the authority considers relevant. (Legislative Council of Hong Kong)

Obligations on CI operators (Part 4)

Category structure (definitions)

- **Category 1 obligation:** an obligation in **Division 1 of Part 4** (Legislative Council of Hong Kong)
- **Category 2 obligation:** an obligation in **Division 2 of Part 4** (Legislative Council of Hong Kong)
- **Category 3 obligation:** an obligation in **Division 3 of Part 4** (Legislative Council of Hong Kong)

Category 1 obligations (examples)

Section 19 — Office in Hong Kong / contact means: CI operator must **maintain an office in Hong Kong** and **provide the regulating authority** with (among other items) the **address**, and the **means** by which the operator may be contacted. (Legislative Council of Hong Kong)

Section 21 — Computer-system security management unit: CI operator must **establish a unit** (however described) responsible for computer-system security of critical computer systems and must provide specified particulars to the regulating authority. (Legislative Council of Hong Kong)

Category 2 obligations (management plan + change notification + risk assessment + audit)

Section 22 — Notify certain events within 1 month: if events listed in section 22(2) occur (including material change to design/configuration/security/operation of a critical computer system; removal of a critical computer system; adding an accessible system essential to core function; or change making an existing accessible system essential to core function), the CI operator must **notify** the regulating authority **within 1 month** of the event. (Legislative Council of Hong Kong)

Section 23 — Submit & implement a computer-system security management plan (3 months): CI operator must submit the plan **within 3 months after the operator's designation date** (extendable on application), and implement it; the plan must cover all matters in **Schedule 3**; revisions must be submitted **within 1 month** of revision. (Legislative Council of Hong Kong)

Section 24 — Risk assessments (first within 12 months; then annually):

- first risk assessment: **within 12 months** after designation date;
- subsequent: **at least once every 12 months** after expiry of the first period;
- report to regulator: **within 3 months** after expiry of the period for conducting the assessment (extendable on application). (Legislative Council of Hong Kong)

Section 25 — Audits (first within 24 months; then every 24 months):

- first audit: **within 24 months** after designation date;
- subsequent: **at least once every 24 months** after expiry of the first period;
- report to regulator: **within 3 months** after expiry of the period for carrying out the audit (extendable on application). (Legislative Council of Hong Kong)

Category 3 obligations (drills + emergency response plan + incident reporting)

Section 26 — Participation in drills: Commissioner may require a CI operator to participate in a computer-system security drill (after reasonable notice). (Legislative Council of Hong Kong)

Section 27 — Emergency response plan (3 months): CI operator must submit an emergency response plan to the Commissioner **within 3 months** after designation date (extendable on application), revisions within **1 month**, and must implement the plan; the plan must cover matters in **Part 2 of Schedule 3**. (Legislative Council of Hong Kong)

Section 28 — Notify incidents + follow-on written report (Schedule 6 times):

- notification must be made "as soon as practicable" and **within the specified time**;
- if initial notice not in specified form/way, a written record must be submitted;
- CI operator must further submit a written report within the specified time. (Legislative Council of Hong Kong)

Schedule 6 — specified times (examples shown in the schedule table):

- **within 12 hours** in the circumstances set out in item 1(a);
- **within 48 hours** in item 1(b);
- **within 14 days** for the written report in item 2. (Legislative Council of Hong Kong)

HEALTH

There is **one explicit health-specific element** in the Ordinance, and the rest is written in **sector-neutral** terms.

1. **Healthcare is explicitly a "sector" for CIs**
   - **Schedule 1** lists **"Healthcare services"** as a **sector specified for the definition of "critical infrastructure."** (Legislative Council of Hong Kong)
2. **No health-specific "designated authority" is listed**
   - **Schedule 2** specifies designated authorities for only:
     - **Monetary Authority** — sector: **Banking and financial services**
     - **Communications Authority** — sector: **Telecommunications and broadcasting services** (Legislative Council of Hong Kong)
3. **Obligations are framed for "CI operators" generally (not a health-only sub-regime)**
   - The Ordinance structures compliance as **"Part 4 — Obligations of CI Operator"** (with Divisions for organization, prevention, and incident reporting/response). (Legislative Council of Hong Kong)

So, the **health-specific hook** is the inclusion of **"Healthcare services"** in **Schedule 1**; the remaining designation/obligation machinery is expressed at the **CI operator / critical computer system** level. (Legislative Council of Hong Kong)

References (Hong Kong)

1. **Legislative Council of Hong Kong. Protection of Critical Infrastructures (Computer Systems) Ordinance (Ord. No. 4 of 2025).** (LegCo)

2. **Communications Authority. Hong Kong Government: PCICSO Commencement Notice.** (link)

ISRAEL

Final categories (what is "highest critical / protected")

1. **"הגבוהה האבטחה רמת עליהם שחלה מאגרים"** ("databases to which the **high security level** applies") — **Protection of Privacy Regulations (Data Security), 5777–2017** (הגנת תקנות הפרטיות (מידע אבטחת), תשע"ז–2017).

2. **"חמור אבטחה אירוע"** ("**severe security incident**") — defined in **Protection of Privacy Regulations (Data Security), 5777–2017**.

3. (Additional legal category used for public bodies' security duties): **"אבטחה פעולות"** ("security actions"), explicitly including **information-security-related activity** — **Law for Regulating Security in Public Bodies, 5758–1998** (חוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח–1998).

Exact legal / regulatory criteria (what triggers inclusion)

Subsection A (The Definition): the specific text defining the scope

1) Database security levels (basic / medium / high) — definitions (Data Security Regulations, 2017):

- **"הבסיסית האבטחה רמת עליהם שחלה מאגרים"** — databases **not** listed in the First or Second Schedule and not managed by an individual.
- **"הבינונית האבטחה רמת עליהם שחלה מאגרים"** — databases of the types listed in the **First Schedule** (and not managed by an individual).
- **"הגבוהה האבטחה רמת עליהם שחלה מאגרים"** — databases of the types listed in the **Second Schedule**.

2) Severe security incident ("חמור אבטחה אירוע") — definition (Data Security Regulations, 2017):

- For a **high-security-level** database: "אירוע שנעשה בו שימוש במידע מן המאגר, בלא הרשאה או בחריגה מהרשאה או שנעשתה פגיעה בשלמות המידע" (unauthorized use / use beyond authorization, or integrity impairment).
- For a **medium-security-level** database: "אירוע שנעשה בו שימוש בחלק מהותי מן המאגר..." (unauthorized use / beyond authorization, or integrity impairment **regarding a substantial part of the database**).

3) Public-body security actions include information-security actions (Security in Public Bodies Law, 1998):

- "אבטחה פעולות" includes "פעילות לאבטחת מידע שחשיפתו עלולה לפגוע בבטחון המדינה" (activity to secure information whose exposure may harm state security).

Subsection B (The Thresholds): quantitative or qualitative tests

Severe security incident thresholds are explicitly differentiated by the database's security level:

- **High level**: unauthorized use (or beyond authorization) of **information from the database**, or **integrity impairment** (no "substantial part" qualifier).
- **Medium level**: unauthorized use (or beyond authorization) of a **"מהותי חלק"** ("substantial part") of the database, or integrity impairment regarding a substantial part.

Grading / tiering scheme

Tiered scheme (3 levels) under the Data Security Regulations:

- **Basic / Medium / High security level** categorization for databases, defined via inclusion in the First / Second Schedules (and exclusions for individually managed databases).

Incident reporting tests and thresholds

Deadlines: 24-hour / 72-hour rules

No 24h/72h deadline text located in the accessible primary regulatory text used below (Data Security Regulations). The regulation uses **"מיידי באופן"** ("immediately") for notification to the Registrar in the severe-incident case.

Triggers: what counts as a reportable incident

Trigger + duty (Data Security Regulations, Regulation 11(ד)):

- "אירע אירוע אבטחה חמור – (1) יודיע על כך בעל המאגר לרשם באופן מיידי..."

  (If a severe security incident occurred — (1) the database owner shall notify the Registrar **immediately**...).

Registrar-directed notification to data subjects (Data Security Regulations, Regulation 11(ד)(2)):

- The Registrar may instruct the database owner (with certain statutory exceptions) — **after consulting** the head of the national cyber authority ("ראש הרשות הלאומית להגנת הסייבר") — to notify affected data subjects ("נושא מידע").

Health information systems "most likely" designated

What is explicit in accessible primary sources

Healthcare entities referenced as part of "health organizations" (State Comptroller report):

- The State Comptroller report cites a Ministry of Health definition of **"ארגון בריאות"** ("health organization") including: the Ministry of Health, health funds (HMOs), medical institutions (including hospitals), pharmacies, evacuation and rescue organizations, clinics, and other organizations licensed by the Ministry of Health.

Databases that include information subject to professional confidentiality are explicitly carved out from the "individually managed database" category (Data Security Regulations):

- "אתיקה של עקרונות לפי או דין לפי מקצועית סודיות לחובת בשלו כפוף המאגר שבעל מידע הכולל מידע מאגר" (a database including information subject to professional confidentiality by law or professional ethics).

Evidence-based inference

Based on (a) the explicit scope of "health organizations" above and (b) the Data Security Regulations' database-security-level framework, examples of **health-sector information systems that commonly operate as "databases" containing professionally confidential health information** include: **EHR/EMR databases, hospital information systems, laboratory information systems, radiology/PACS archives, pharmacy systems, appointment & admissions systems, emergency dispatch/ambulance care records, and national/regional registries**.

This list is **not** a designation list from Israeli law; it is an inference about typical systems that store the regulated classes of information described above.

Public vs Confidential

Public (located and cited):

- **Security in Public Bodies Law (1998)** — statutory definitions including "security actions" that explicitly include securing sensitive information whose exposure may harm state security.
- **Protection of Privacy Regulations (Data Security) (2017)** — definitions of security levels; definition of "severe security incident"; immediate notification duty to the Registrar; possible Registrar-directed notification to data subjects after consultation with the national cyber authority.

Confidential (not contained in the accessible legal texts above):

- The cited laws/regulations above **do not themselves publish a list** of specific designated entities or systems as "critical infrastructure." (No such list appears within the cited sections of the statutes/regulations.)

Latest updates (2025–2026)

- **Privacy Protection Law (Amendment No. 13), 2024** (חוק הגנת הפרטיות (תיקון מס' 13), התשפ"ד–2024) was published in Israel's Book of Laws ("ספר החוקים") on **14 Aug 2024** and is identified as Amendment No. 13 in that publication.
- Accessible sources discussing commencement state that **Amendment 13 enters into force on 14 Aug 2025** (one year after publication).

References (Israel)

1. **The Knesset. Regulation of Security in Public Bodies Law, 5758–1998** (חוק להסדרת הביטחון בגופים ציבוריים). (link)
2. **Israel Privacy Protection Authority. Protection of Privacy Regulations (Data Security), 5777–2017**. (English translation)
3. **State Comptroller of Israel. Annual Report: Healthcare Cybersecurity**. (link)

4. **The Knesset. Privacy Protection Law (Amendment No. 13), 2024**. (link)

Part 2: Comparative Synthesis & Framework Design Recommendations

Comparative Framework Overview

This study provides deep-dive analysis of **17 jurisdictions** with detailed chapter coverage, plus an additional **20+ countries** surveyed in the multi-region overview table.

Deep-Dive Jurisdictions (17 Countries)

Country/Region	Designation Model	Transparency	Explicit Thresholds	2025-2026 Updates
USA	Sector-level (HPH sector)	Frameworks public, priorities confidential	No (voluntary, qualitative)	**CIRCIA final rule expected (May 2026), 72-hr incident/24-hr ransom reporting**
Australia	Asset-level (ICU hospitals)	Criteria fully public, SoNS confidential	**Yes (ICU presence)**	**Ransomware payment reporting (May 2025), strict enforcement (Jan 2026)**
EU (NIS2)	Entity-level (Essential/Important)	Criteria fully public, lists vary by state	**Yes (≤50 employees, €10M)**	**CER Directive (July 2026 deadline), all-hazard resilience**
Canada	Sector-based (10 CI sectors)	CI definition public	No (qualitative)	**Bill C-8/CCSPA proposed (72-hr reporting)**
UK	Entity-level (OES)	Criteria public, lists confidential	**Yes (incident thresholds most explicit globally)**	**Cyber Security Bill (Nov 2025), expands to MSPs/suppliers, 24-hr reporting**
Germany	System/entity (KRITIS + NIS2)	**High (thresholds public)**	**Yes (30,000 inpatient cases/year)**	NIS2 implementation law in force (6 Dec 2025)
Singapore	System-level (individual CII)	Criteria public, lists confidential	No (qualitative "debilitating")	No major updates

Country/Region	Designation Model	Transparency	Explicit Thresholds	2025-2026 Updates
New Zealand	Risk-based (HISO segmentation)	Partially public	No (qualitative, developing)	**PSR GOV framework (1 Oct 2025)**
Japan	Entity-level (discretionary)	Medium (hospital categories public)	No (qualitative "excluding small scale")	No major updates
China	System/entity (CII + MLPS)	Low (general criteria only)	No (party-state discretion)	No major updates
South Korea	Designation-based (CIIC)	**High (Official Gazette publication)**	No (5-factor qualitative test)	No major updates
France	Entity-level (OIV/SAIV)	Criteria public, lists confidential	No (qualitative)	No major updates
Norway	Entity-level (socially important services)	Criteria public	No (qualitative "significantly disruptive")	**Digital Security Act in force (1 Oct 2025), 24h/72h reporting**
Switzerland	Entity-level (CI operators)	Criteria public, entities via permits	No (qualitative, category-based)	**Cybersecurity Ordinance (CSV) in force (1 Apr 2025), 24h reporting**
Taiwan	Designation-based (CI providers)	Criteria public	No (administrative designation)	**CSMA revised (24 Sept 2025), MoDA as authority**
Thailand	Designation-based (CII orgs)	Criteria public (Gazette)	No (Committee notification)	No major updates cited
Hong Kong	Designation-based (CI operators)	**High (criteria + obligations public)**	No (qualitative "essential to core function")	**CI Ordinance in force (1 Jan 2026), 12h/48h/14d reporting**
Israel	Database security levels	Criteria public	**Yes (3-tier: Basic/Medium/High)**	**Privacy Law Amendment 13 effective (14 Aug 2025)**

Universal Health Information Systems Prioritized Globally

Across all 17 deep-dive jurisdictions, consistent prioritization emerges for:

1. **Emergency call-taking and ambulance dispatch** (111/112/119/911/999 + Computer Aided Dispatch)

2. **Major hospital core clinical systems** (EMR/EHR, EDIS, ICU monitoring)

3. **Intensive care unit systems** (explicitly: Australia, UK, Germany; implicitly: all others)

4. **Blood bank and transfusion services** (national/regional level)

5. **National/regional infectious disease surveillance**

6. **National health information infrastructure** (where exists: electronic prescription, national EHR)

High but variable priority:

7. Ambulance electronic patient care records (ePCR/ePRF)

8. Operating theatre management and anesthesia systems

9. Hospital laboratory information systems (LIMS)

10. Pharmacy management and ePrescribing (hospital-based)

11. Medical imaging systems (PACS/RIS in acute settings)

12. National immunization registries

13. Organ and tissue transplant allocation systems

Lower priority (but still important):

- Community hospital systems (if alternatives exist)

- Primary care / GP systems (unless sole provider)

- Outpatient specialty clinics

- Health research systems (non-pandemic)

- Administrative/billing systems

Emerging Global Trends (2025-2026)

Key Regulatory Milestones (2025-2026)

Date	Jurisdiction	Milestone
1 Apr 2025	Switzerland	Cybersecurity Ordinance (CSV) enters into force; 24-hour reporting
30 May 2025	Australia	Mandatory ransomware payment reporting in effect
14 Aug 2025	Israel	Privacy Protection Law Amendment 13 enters into force
24 Sept 2025	Taiwan	Revised Cyber Security Management Act promulgated
1 Oct 2025	Norway	Digital Security Act and Regulations enter into force
1 Oct 2025	New Zealand	PSR GOV Policy Framework implemented
Nov 2025	UK	Cyber Security and Resilience Bill introduced
6 Dec 2025	Germany	NIS2 implementation law (NIS2UmsuCG) enters into force
1 Jan 2026	Australia	Strict enforcement posture begins
1 Jan 2026	Hong Kong	Protection of Critical Infrastructures Ordinance enters into force
May 2026	USA	CIRCIA final rule expected
17 July 2026	EU	CER Directive deadline for identifying critical entities

1. Supply Chain Regulation Expansion

- **UK**: New Bill explicitly targets **Managed Service Providers (MSPs)** and **critical suppliers**

- **EU**: NIS2 includes manufacturers of medical devices and pharmaceuticals

- **Implication**: Future frameworks must include criteria for assessing and mandating security standards for third and fourth-party vendors

2. All-Hazard Resilience Integration

- **EU CER Directive**: Mandates resilience plans for physical, environmental, natural disaster, and supply chain disruptions

- **Shift**: Moving beyond pure cybersecurity to require planning for broader disruptions that could impact digital services

- **Implication**: Critical infrastructure frameworks should integrate business continuity planning for multi-hazard scenarios

3. Stricter & Harmonized Incident Reporting

Global convergence towards standardized reporting timelines:

Reporting Stage	Common Standard	Examples
Early warning	12-24 hours	Hong Kong (12h), Norway (24h), Switzerland (24h), EU NIS2 (24h)
Detailed notification	48-72 hours	Hong Kong (48h), Norway (72h), EU NIS2 (72h), USA CIRCIA (72h)
Final report	14-30 days	Hong Kong (14d), Norway (1 month), EU NIS2 (1 month)
Ransom payment	24 hours	USA CIRCIA, Australia

4. Enhanced Enforcement Postures

- **Australia**: Shift to "stricter enforcement-oriented posture" from January 2026

- **EU**: Significant penalties (up to €10M or 2% global turnover)

- **Hong Kong**: Fines up to HK$5M for non-compliance with CI operator obligations
- **Implication**: Compliance moving from voluntary guidance to mandatory requirement with serious consequences for non-compliance

Key Policy Design Insights for New Jurisdictions

This section synthesizes lessons learned from the 17 jurisdictions analyzed, organized as actionable decision points for policymakers.

Designation Model Trade-offs

Model	Advantages	Disadvantages	Best For	Examples
Sector-based (no designation)	Low administrative burden; covers all entities in sector	Lacks precision; may burden small providers unnecessarily	Countries with limited regulatory capacity	USA, Canada
Entity-based designation	Clear accountability; scales with organization	May miss critical small providers	Developed regulatory systems	UK (OES), EU (NIS2), France (OIV)
System-based designation	Precise; focuses on actual critical systems	Complex to administer; requires technical assessment	High IT maturity jurisdictions	Singapore (CII)
Asset-based designation	Clear thresholds; easy to verify	May be too rigid; misses critical functions at smaller sites	Jurisdictions wanting explicit rules	Australia (ICU hospitals), Germany (30k cases)
Hybrid	Flexible; covers edge cases	More complex to implement	Most jurisdictions moving this direction	Germany (KRITIS + NIS2), Hong Kong

> **Recommendation for new countries:** Start with **sector + entity-based** for broad coverage, then add **system/asset thresholds** as regulatory capacity matures.

Which Health Entities to Include (Global Consensus)

Based on analysis across all 17 jurisdictions, the following entities appear most frequently in CI/CII frameworks:

Tier 1: Near-Universal Inclusion (explicitly included in 80%+ of frameworks)

Entity Type	Notes	Example Jurisdictions
Hospitals with ICU/emergency capability	Often defined by bed count or case volume	Australia, Germany, UK, EU, Hong Kong
National/regional health information exchanges	EHR platforms, health data networks	Singapore, Japan, Taiwan
Blood and organ allocation services	Often at national level	Germany, France, UK
Disease surveillance systems	Epidemic response capability	All jurisdictions (explicitly or implicitly)
Emergency ambulance dispatch (CAD)	Often in "emergency services" sector	UK, EU, Australia

Tier 2: Frequently Included (50-80% of frameworks)

Entity Type	Notes	Example Jurisdictions
Medical laboratories (reference/diagnostic)	Often linked to epidemic response	Switzerland, EU, Germany
Pharmaceutical manufacturers/distributors	Supply chain criticality	EU (NIS2), Germany
Medical device manufacturers	Especially IVD and implantables	EU (NIS2 Annex II), Germany
National immunization registries	Pandemic preparedness	Japan, Taiwan

Tier 3: Variable Inclusion (depends on national context)

Entity Type	Notes	Jurisdictions with Explicit Inclusion
Private hospital chains	Based on market share or regional importance	Singapore, Hong Kong

Entity Type	Notes	Jurisdictions with Explicit Inclusion
Telehealth platforms	Emerging; few explicit designations yet	None explicitly (emerging area)
Health insurance claims systems	Administrative criticality	USA (implicit), Germany

Governance Structure Options

Structure	Description	Pros	Cons	Examples
Centralized cyber agency	Single agency designates and supervises all CI	Consistency; clear accountability	May lack health sector expertise	Singapore (CSA), Israel (INCD)
Sector-specific regulator	Health ministry/agency handles health CI	Domain expertise; existing relationships	May lack cyber expertise; fragmentation	Japan (MHLW), France (health ministry)
Hybrid with sector leads	Central cyber coordination; sector authorities designate	Balances expertise; coordination	Complexity; inter-agency friction	UK, Germany, Hong Kong
Federated (federal countries)	Shared federal/state responsibility	Respects local context	Coordination challenges; gaps	Canada, Australia, Germany

Recommendation for new countries: Hybrid model with a central cybersecurity coordination body and sector-specific designation authority in the health ministry tends to balance expertise best.

Threshold Design: Quantitative vs Qualitative

Approach	Description	When to Use	Examples
Explicit quantitative	Numeric thresholds (beds, cases, employees)	High data availability; desire for predictability	Germany (30,000 cases/yr), EU (≤50 employees), Australia (ICU presence)

Approach	Description	When to Use	Examples
Qualitative + factors	Multi-factor assessment; committee review	Lower data availability; diverse health system	South Korea (5-factor test), Singapore ("debilitating effect")
Functional designation	Based on services provided, not size	Small but critical providers (e.g., sole provider in region)	EU ("regardless of size" exceptions), UK, NZ
Registration-based	Entities self-assess and register; spot-check enforcement	Resource-constrained regulators	Germany (NIS2 registration), Hong Kong

Key insight from global analysis: Pure quantitative thresholds miss edge cases. Best practice combines a quantitative baseline with qualitative "safety net" criteria (e.g., "sole provider," "unique capability," "cross-border impact").

Common Implementation Pitfalls (Lessons from Established Frameworks)

Pitfall	Lesson Learned	Countries with This Issue
Confidential lists become stale	Build in mandatory periodic review (e.g., every 2 years)	EU (mandates 2-year review), UK
Small critical providers overlooked	Include "regardless of size" exceptions for unique/sole providers	EU NIS2, UK
Supply chain not covered	Explicitly include MSPs, cloud providers, medical device vendors	UK (new Bill), EU
No escalation path for evolving threats	Build in mechanism for emergency temporary designation	Taiwan, South Korea
Reporting burden on small providers	Tiered reporting obligations proportionate to size/criticality	EU (Essential vs Important), Israel (3-tier)
Siloed from other CI sectors	Map and address interdependencies (power, telecom, water)	Most mature frameworks address this

What to Make Public vs Confidential

Element	Global Consensus	Rationale
Designation criteria	**PUBLIC**	Enables self-assessment; transparency; predictability
Reporting thresholds	**PUBLIC**	Clear compliance expectations
List of designated entities	**CONFIDENTIAL**	Avoid creating target list for attackers
Aggregate statistics	**PUBLIC (anonymized)**	Sector learning; accountability
Incident reports	**CONFIDENTIAL** (individual); **PUBLIC** (aggregated/anonymized)	Balance learning vs security

South Korea exception: Official Gazette publication of designated CII is required by law, demonstrating that transparency models can work with appropriate security measures.

Updated Recommendations for Framework Design (2025-2026)

Based on comprehensive analysis and latest global developments:

1. Adopt Hybrid Criticality Criteria

- **Combine Approaches**: Use explicit thresholds (like Germany's 30,000 cases, Australia's ICU presence) for objectivity, supplemented by qualitative assessment for unique critical providers.

- **Include Supply Chain**: Explicitly incorporate MSPs and critical suppliers in scope (following UK model).

- **Functional + Size-Based**: Combine functional designations (emergency services, blood/organ systems) with size-based thresholds (EU's ≥50 employees).

2. Implement Proportional Three-Tier System

- **Tier 1 (Essential/Critical)**: Highest obligations, ex-ante supervision, 24/7 monitoring requirements

- **Tier 2 (Important)**: Moderate obligations, ex-post supervision, regular assessments

- **Tier 3 (Baseline)**: Basic cyber hygiene, voluntary reporting

- **Align Penalties**: Proportionate penalties based on tier and organizational size

3. Establish Clear Incident Reporting Thresholds

- **Adopt UK-Style Metrics**: Implement explicit, quantitative incident thresholds (patient counts, service disruption durations)

- **Harmonize Timelines**: Align with emerging global standards (24-hour initial, 72-hour detailed)

- **Special Ransomware Reporting**: Consider mandatory ransom payment reporting within 24 hours

4. Ensure Strategic Transparency

- **Public Criteria**: Publish clear designation criteria enabling self-assessment

- **Confidential Lists**: Maintain confidential entity lists to avoid creating target lists

- **Aggregate Reporting**: Publish anonymized sector statistics and case studies for learning

5. Integrate All-Hazard Resilience

- **Beyond Cybersecurity**: Require business continuity and disaster recovery planning for physical, environmental, and supply chain disruptions

- **Regular Testing**: Mandate annual or biennial testing of resilience plans

- **Cross-Sector Dependencies**: Map and address interdependencies with other critical infrastructure sectors
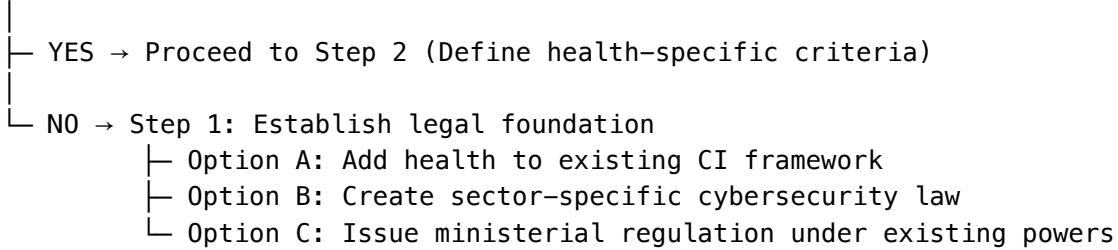
6. Future-Proof for Emerging Technologies

- **Telehealth Platforms**: Explicitly include national/regional telehealth systems

- **AI/ML Systems**: Consider criticality of AI-driven diagnostic and treatment systems

- **IoT Medical Devices**: Address security of connected medical device ecosystems

Implementation Roadmap for New Jurisdictions

Quick-Start Decision Tree

```
START: Is health explicitly listed as a CI sector in existing national law?
    │
    ├─ YES → Proceed to Step 2 (Define health-specific criteria)
    │
    └─ NO → Step 1: Establish legal foundation
              ├─ Option A: Add health to existing CI framework
              ├─ Option B: Create sector-specific cybersecurity law
              └─ Option C: Issue ministerial regulation under existing powers
```

Model Legislation Elements (Based on Global Best Practices)

Element	Recommended Approach	Reference Models
Definition of "health CI"	Entity-based + functional criteria	EU NIS2 (healthcare providers), Australia (ICU hospitals)
Designation authority	Health ministry with cybersecurity agency coordination	Hong Kong, Germany, UK
Scope criteria	Quantitative baseline + qualitative exceptions	Germany + EU hybrid
Obligations structure	Tiered (Essential/Important or Tier 1/2/3)	EU NIS2, Israel
Incident reporting	24h early warning / 72h detailed / 30d final	EU NIS2, Norway, Hong Kong
Penalties	Proportionate to size; administrative fines + compliance orders	EU, Hong Kong
Review cycle	Mandatory 2-year review of designated list	EU NIS2

Phase 1: Foundation (Months 1-6)

1.1 Legal Authority Assessment

☐ Review existing cybersecurity/CI laws for health sector applicability
☐ Identify gaps requiring new legislation vs ministerial regulation
☐ Map existing health sector regulatory bodies and their powers

1.2 Sector Risk Assessment

☐ Inventory major health information systems in the country
☐ Identify single points of failure (sole providers, national systems)
☐ Assess current incident reporting and cyber hygiene baseline

1.3 Stakeholder Mapping

☐ Identify designated authority (cybersecurity agency, health ministry, or hybrid)
☐ Map hospitals, labs, insurers, technology vendors in health sector
☐ Establish working group with sector representatives

Phase 2: Design & Consultation (Months 7-12)

2.1 Develop Designation Criteria

☐ Define quantitative thresholds (e.g., bed count, case volume, employee count)
☐ Add qualitative safety-net criteria (sole provider, unique capability)
☐ Draft "regardless of size" exception triggers

2.2 Draft Obligations Framework

☐ Tier 1 (Essential): Risk management plan, security officer, 24h reporting, annual audit
☐ Tier 2 (Important): Risk management, 72h reporting, biennial assessment
☐ Tier 3 (Baseline): Basic cyber hygiene, voluntary reporting

2.3 Stakeholder Consultation

☐ Publish draft framework for public comment
☐ Conduct workshops with hospital associations, health IT vendors
☐ Align with telecom, energy, finance CI frameworks on cross-sector issues

Phase 3: Pilot Implementation (Months 13-18)

3.1 Pilot Designation

☐ Designate 5-10 largest/most critical entities for pilot
☐ Test designation process and notification procedures
☐ Refine criteria based on pilot feedback

3.2 Develop Operational Guidance

☐ Create sector-specific security controls guidance (reference: Germany B3S, UK CAF)
☐ Develop incident reporting forms and submission system
☐ Establish information-sharing mechanisms (CERT, sectoral ISAC)

3.3 Capacity Building

☐ Train designated entities on compliance requirements
☐ Train regulatory staff on supervision and enforcement
☐ Establish help desk for compliance questions

Phase 4: Full Implementation (Months 19-24)

4.1 Full Rollout

☐ Designate all in-scope entities based on final criteria
☐ Activate mandatory incident reporting
☐ Begin compliance monitoring

4.2 Enforcement Framework

☐ Establish graduated enforcement (warning → compliance order → fine)
☐ Publish anonymized enforcement statistics for sector learning
☐ Create appeals/review mechanism

4.3 Cross-Sector Integration

☐ Map interdependencies with power, telecom, water CI
☐ Establish joint incident response protocols
☐ Participate in national/regional CI coordination mechanisms

Phase 5: Maturity & Evolution (Ongoing)

5.1 Continuous Improvement

☐ Conduct annual review of designation criteria effectiveness
☐ Update thresholds based on sector evolution (e.g., telehealth growth)
☐ Incorporate lessons from incident response

5.2 International Alignment

☐ Monitor and align with regional frameworks (EU NIS2, ASEAN, etc.)
☐ Participate in international information-sharing networks
☐ Consider mutual recognition agreements for cross-border operators

5.3 Emerging Technology Integration

☐ Add AI/ML diagnostic systems to scope consideration
☐ Address IoT medical device security
☐ Update for cloud and SaaS health platforms

Conclusion

This comprehensive analysis of **17 jurisdictions** with detailed chapter coverage, plus an additional **20+ countries** surveyed across Latin America, ASEAN, Africa, Middle East, and Central Asia, reveals a global landscape undergoing significant transformation in 2025-2026. **Five key trends dominate:**

1. **Expanded Scope**: Regulations now explicitly encompass supply chains, with MSPs and critical suppliers facing direct obligations (UK, EU).

2. **Holistic Resilience**: The shift from pure cybersecurity to all-hazard resilience planning (EU CER Directive) reflects recognition that health systems face multifaceted threats.

3. **Stricter Reporting**: Convergence towards 12-24 hour early warning and 48-72 hour detailed notification, with specific ransomware payment reporting (24 hours in USA, Australia).

4. **Enhanced Enforcement**: Moving from voluntary guidance to mandatory requirements with significant penalties (EU up to €10M, Hong Kong up to HK$5M).

5. **New Jurisdictions Entering the Framework**: 2025-2026 sees major new entrants including Hong Kong (CI Ordinance), Switzerland (CSV), Norway (Digital Security Act), and Taiwan (revised CSMA).

Despite diverse legal traditions and cultural contexts, remarkable consensus exists on which health systems merit highest protection: emergency services, major hospital clinical systems, blood/organ services, and disease surveillance platforms. The most effective frameworks emerging from this global analysis combine **transparent, objective criteria** (enabling self-assessment) with **proportionate, risk-based obligations** (ensuring appropriate resource allocation), while maintaining necessary **confidentiality over specific asset lists** (preserving security). For jurisdictions developing or updating their health critical infrastructure frameworks, the 2025-2026 updates from the UK, EU, US, Australia, Hong Kong, Switzerland, and Norway provide a clear roadmap emphasizing supply chain security, all-hazard resilience, and harmonized incident reporting. These developments, coupled with the foundational principles from established frameworks like Germany's precise thresholds, Singapore's system-level approach, and South Korea's transparent designation process, create a comprehensive model for protecting the digital foundations of healthcare in an increasingly interconnected and threatened world.

References (Global Synthesis)

1. **Cyber Security Agency of Singapore (CSA). Cybersecurity Act**. (CSA)
2. **Cyber Security Agency of Singapore (CSA). Code of Practice for Critical Information Infrastructure Protection (Second Edition)**. (CSA)
3. **Cyber Security Agency of Singapore (CSA). Healthcare Cybersecurity Masterplan 2021-2023**.
4. **Australian Government. Security of Critical Infrastructure Act 2018**. (Legislation.gov.au)
5. **Australian Government, Department of Home Affairs. Security of Critical Infrastructure (Definitions) Rules 2021**.
6. **Australian Government, Department of Home Affairs. Security of Critical Infrastructure (Risk Management Program) Rules 2023**.
7. **Critical Infrastructure Centre. SOCI Act 2018 for healthcare and medical**. (CISC)

8. UK Parliament. **The Network and Information Systems Regulations 2018 (SI 2018/506)**. (Legislation.gov.uk)

9. UK Department of Health and Social Care. **The Network and Information Systems Regulations 2018: guide for the health sector in England**. (GOV.UK)

10. UK National Cyber Security Centre. **Cyber Assessment Framework (CAF)**. (NCSC)

11. European Parliament and Council. **Directive (EU) 2022/2555 (NIS2 Directive)**.

12. European Commission. **FAQs on NIS2 Directive**. (European Commission)

13. European Commission. **Infringement proceedings for non-transposition of NIS2**. (European Commission)

14. The White House. **Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience**.

15. Cybersecurity and Infrastructure Security Agency (CISA). **National Critical Functions**. (CISA)

16. U.S. Department of Health and Human Services. **Health Industry Cybersecurity Practices (HICP)**. (405d.hhs.gov)

17. U.S. Department of Health and Human Services. **HIPAA Security Rule**. (HHS.gov)

18. National Conference of State Legislatures. **State Critical Infrastructure Laws**. (NCSL)

19. U.S. Government Accountability Office. **Federal Health Cybersecurity**. ([GAO][19])

20. Public Safety Canada. **National Strategy for Critical Infrastructure**. ([Public Safety Canada][20])

21. Ontario Ministry of Health. **Emergency Management Framework for Health**. ([Ontario.ca][21])

22. Canadian Centre for Cyber Security. **Cyber Incident Management for Canada's Health Sector**. ([Cyber.gc.ca][22])

23. New Zealand Government. **Computer Emergency Response Team Act 2016**.

24. Te Whatu Ora - Health New Zealand. **Cybersecurity and Critical Infrastructure Framework (Draft)**.

25. Bundesamt für Sicherheit in der Informationstechnik (BSI). **BSI-KritisV and IT-Sicherheitsgesetz 2.0**. ([BSI][25])

26. Bundesministerium des Innern und für Heimat. **NIS2-Umsetzungsgesetz (NIS2UmsuCG)**. ([BMI][26])

27. National center of Incident readiness and Strategy for Cybersecurity (NISC), Japan. **Cybersecurity Basic Act and Policy Guidelines**. ([NISC][27])

28. Ministry of Health, Labour and Welfare (MHLW), Japan. **Healthcare Information System Security Guidelines**. ([MHLW][28])

29. Personal Information Protection Commission, Japan. **Health Data Breach Reporting**. ([PPC][29])

30. National People's Congress, China. **Cybersecurity Law of the People's Republic of China**.

31. State Council, China. **Critical Information Infrastructure Security Protection Regulations**.

32. Ministry of Public Security, China. **Multi-Level Protection Scheme 2.0 Standards**.

33. National Health Commission, China. **Health Critical Information Infrastructure Protection Guidelines**.

34. Cyberspace Administration of China. **CII Security Incident Reporting Requirements**. ([CAC][34])

Health as a Critical Information / Critical Infrastructure Sector

Region	Country	Status (health as CI/CII sector)	Ref(s)
Latin America	Chile	**Explicit (primary):** "prestación institucional de servicios de salud" listed as an **essential service** under the national cybersecurity/critical infrastructure framework	1
	Mexico	**Not confirmed (primary not found in accessible sources):** I did not find a government text explicitly listing "health/healthcare" as a CI/CII sector in the sources retrieved for this run	—
ASEAN	Singapore	**Explicit (primary):** CSA lists **Healthcare** among **CII sectors** under the Cybersecurity Act	2
	Malaysia	**Explicit (primary):** NACSA lists **Healthcare Services** as an NCII sector	3
	Indonesia	**Explicit (primary):** official summary of **Perpres 82/2022** lists **Sektor kesehatan** as a strategic sector for Vital Information Infrastructure protection	4
	Thailand	**Explicit (secondary):** "Public Health" presented as a CII sector under Thailand's Cybersecurity Act (source is not a government statute page)	5
Africa	Ghana	**Explicit (primary):** CSA directive lists **Health** as a Critical Information Infrastructure sector	6
	Kenya	**Explicit (primary):** national coordination body list includes **health** among CII sectors	7
	Nigeria	**Explicit (primary):** national cybersecurity policy/strategy text includes **Public Health and Healthcare Sector**	8
	Egypt	**Not confirmed (primary not found in accessible sources):** a strategy launch page was found, but the **sector list including health** was not located in an accessible primary document in this run	9
Middle East	Bahrain	**Explicit (primary/official):** National Cybersecurity Center lists **Health Services** as a CNI sector	10
	Qatar	**Not confirmed (primary not found in accessible sources):** I only retrieved a news report about the strategy launch (no official sector list including health found in this run)	11
	United Arab Emirates (UAE)	**Explicit (official portal copy):** lists **Health services** among protected critical asset sectors	12
Central Asia	Kazakhstan	**Explicit (primary):** definition/rules for "critical information and communication infrastructure" explicitly include **healthcare**	13
	Kyrgyz Republic	**Explicit (primary):** definition of "critical information infrastructure" includes the field of **healthcare**	14
Southern Africa	Zambia	**Explicit (primary):** Cyber Security Act defines "critical sector" and explicitly includes **health**	15
	Botswana	**Explicit (primary):** national cybersecurity strategy lists critical infrastructure sectors including **health**	16

Region	Country	Status (health as CI/CII sector)	Ref(s)
Eastern Europe	Russia	**Explicit (secondary compilation of legal text):** law scope statement includes systems functioning in the sphere of **healthcare (здравоохранения)**	17
	Ukraine	**Not confirmed (primary not found in accessible sources):** I retrieved official legal portals for "critical infrastructure" concepts, but not an accessible sector list explicitly naming health in this run	18

References (Global Overview)

1. **Government of Chile (Ministerio del Interior / CSIRT Gov). Framework for Essential Services.** (Interior.gob.cl)
2. **Cyber Security Agency of Singapore (CSA). Cybersecurity Act: CII Sectors.** (CSA)
3. **National Cyber Security Agency (NACSA), Malaysia. NCII Sectors Listing.** (NACSA)
4. **Sekretariat Kabinet Republik Indonesia (Setkab). Perpres 82/2022 Summary.** (Setkab.go.id)
5. **Thailand Cybersecurity Act Overview.** (ABB)
6. **Cyber Security Authority, Ghana. CII Sector Directive.** (CSA.gov.gh)
7. **National Cybersecurity Coordination Committee (NC4), Kenya. CII Sector Listing.** (NC4)
8. **ngCERT (Nigeria). National Cybersecurity Policy & Strategy.** (ngCERT)
9. **EG-CERT (Egypt). National Cybersecurity Strategy 2023-2027.** (egcert.eg)
10. **Bahrain National Cybersecurity Center. CNI Sectors List.** (NCSC.gov.bh)
11. **The Peninsula Qatar. Qatar Strategy Launch Report.** (The Peninsula)
12. **UNODC. UAE National Cybersecurity Strategy Summary.** (UNODC)
13. **Republic of Kazakhstan. "Adilet" LIS: CIIC Rules.** (Adilet)
14. **Kyrgyz Republic. Regulation for Information Protection in SIS.** (dpa.gov.kg)
15. **Republic of Zambia. Cyber Security Act, 2025.** (ZambiaLII)
16. **Republic of Botswana. National Cybersecurity Strategy.** (BoCRA)
17. **Kaspersky Regulhub. Russia 187-FZ Scope List.** (Regulhub)
18. **Verkhovna Rada. Official Legal Portal of Ukraine.** (Rada.gov.ua)

Health Sector Critical Information Infrastructure: Metrics and Grading Framework

Introduction

This chapter synthesizes the comprehensive analysis of 17 jurisdictions to define a **metrics-based framework** for identifying and classifying health sector entities as **Critical Information Infrastructure (CII)**. The framework combines quantitative thresholds with qualitative criteria, drawing on global best practices to create a practical, adaptable approach.

Part 1: Designation Metrics

1.1 Quantitative Thresholds (Direct Evidence from Global Frameworks)

Metric Category	Threshold	Jurisdiction Source	Evidence Level
Inpatient case volume	≥30,000 full inpatient cases/year	Germany (BSI-KritisV Anhang 5)	Explicit
ICU presence	Hospital has a general ICU (capable of mechanical ventilation for several days + invasive cardiovascular monitoring)	Australia (SOCI Act 2018)	Explicit
Organization size	≥50 employees OR €10M+ annual turnover	EU NIS2 Directive	Explicit
Laboratory throughput	≥1,500,000 diagnostic tests/year	Germany (BSI-KritisV)	Explicit
Blood/plasma production	≥34,000 products manufactured or marketed/year	Germany (BSI-KritisV)	Explicit
Customer impact (national)	Service loss affecting >100,000 customers	New Zealand (NVA 2023)	Explicit

Metric Category	Threshold	Jurisdiction Source	Evidence Level
Customer impact (regional)	Service loss affecting 20,000–100,000 customers	New Zealand (NVA 2023)	Explicit

1.2 Qualitative Designation Criteria
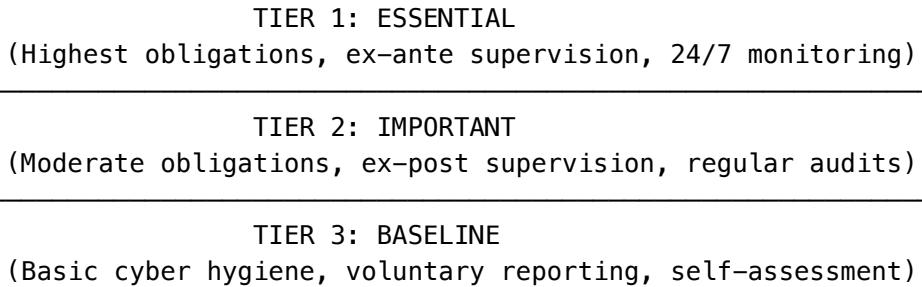
Functional Criticality Criteria (from 17 jurisdictions)

Criterion	Description	Jurisdiction Examples
Sole provider	Entity is the only provider of an essential service in a geographic area	EU NIS2, UK, Singapore
Debilitating effect	System compromise would have a debilitating effect on service availability	Singapore (Cybersecurity Act)
Public health impact	Disruption could seriously affect public health or safety	EU NIS2, Norway, Thailand, France
Cross-border impact	Significant systemic risk with potential cross-border effects	EU NIS2
Life-safety dependency	Direct dependency for life-critical patient care	All 17 jurisdictions
National/regional importance	Critical due to specific importance at national or regional level	EU NIS2, South Korea
Core function essentiality	System is essential to the core function of the infrastructure	Hong Kong
Substitutability	Difficult to substitute or replace	France, Hong Kong

Part 2: Multi-Tier Classification Framework

2.1 Recommended Three-Tier Model

Based on global synthesis, a **three-tier classification** balances precision with administrative feasibility:

```
|                    TIER 1: ESSENTIAL                        |
|      (Highest obligations, ex-ante supervision, 24/7 monitoring)  |
├─────────────────────────────────────────────────────────────┤
|                    TIER 2: IMPORTANT                        |
|      (Moderate obligations, ex-post supervision, regular audits)  |
├─────────────────────────────────────────────────────────────┤
|                    TIER 3: BASELINE                         |
|      (Basic cyber hygiene, voluntary reporting, self-assessment)  |
```

2.2 Tier Definitions and Criteria

TIER 1: Essential (Critical)

Criterion	Threshold/Test	Weight
Quantitative Size	Meets ANY explicit threshold (e.g., ≥30,000 cases/year OR ≥50 employees)	High
ICU/Emergency Capability	Hospital with ICU and/or major trauma/emergency department	High
National System	Operates a national-level health information system	High
Sole Provider	Only provider of essential health service in region	High
Blood/Organ Services	Operates blood bank, organ allocation, or transfusion services at national/regional level	High
Disease Surveillance	Operates infectious disease surveillance at national/regional level	High

Examples of Tier 1 Entities: - Major hospitals with ICU and emergency departments - National/regional health information exchanges (EHR platforms) - National blood and organ allocation services - Disease surveillance and epidemic response systems - Emergency ambulance dispatch systems (CAD) - Class III Grade A hospitals (China terminology)

TIER 2: Important

Criterion	Threshold/Test	Weight
Moderate Size	Employs 10-49 OR €2M-€10M turnover	Medium
Regional Service	Provides essential services at regional/metropolitan level	Medium
Supply Chain Criticality	Key supplier to Tier 1 entities	Medium
Specialty Care	Specialty hospital or referral center	Medium
Diagnostic Services	Medical laboratories (reference/diagnostic)	Medium

Criterion	Threshold/Test	Weight
Pharmaceutical	Pharmaceutical manufacturers/distributors	Medium

Examples of Tier 2 Entities: - Community hospitals without ICU but with significant ED - Reference and diagnostic laboratories - Pharmaceutical manufacturers and distributors - Medical device manufacturers (especially IVD and implantables) - Regional immunization registries - Managed service providers (MSPs) serving health sector

---

TIER 3: Baseline

Criterion	Threshold/Test	Weight
Small Enterprise	<10 employees AND <€2M turnover	Low
Local Service	Provides primarily local/community services	Low
Redundancy Available	Alternative providers exist in the service area	Low
Non-acute Care	Outpatient specialty, primary care, wellness	Low

Examples of Tier 3 Entities: - Primary care/GP clinics (unless sole provider) - Outpatient specialty clinics - Dental practices - Allied health providers - Health research institutions (non-pandemic)

Part 3: Scoring Methodology

3.1 Weighted Scoring Matrix

A **point-based scoring system** translates criteria into tier classification:

Domain	Criterion	Points	Max Points
A. Scale			**30**
	≥30,000 inpatient cases/year	30	
	15,000–29,999 cases/year	20	
	5,000–14,999 cases/year	10	
	<5,000 cases/year	5	
B. Capability			**25**
	General ICU present	25	
	High-dependency unit (no ICU)	15	
	Emergency department only	10	
	No acute care capability	0	
C. Functions			**25**

Domain	Criterion	Points	Max Points
	Emergency dispatch (111/999/911)	25	
	Blood bank/transfusion services	20	
	Disease surveillance (national/regional)	20	
	Organ allocation services	20	
	National EHR/HIE platform	25	
	Regional EHR/HIE platform	15	
D. Uniqueness			**10**
	Sole provider in region	10	
	Unique specialty capability	8	
	Alternative providers available	0	
E. Dependencies			**10**
	Cross-sector dependencies (telecom, power)	10	
	Other health systems depend on this entity	8	
	Limited external dependencies	3	

3.2 Tier Classification Thresholds

Tier	Score Range	Classification
Tier 1	≥60 points	Essential
Tier 2	30–59 points	Important
Tier 3	<30 points	Baseline

3.3 Automatic Tier 1 Triggers ("Regardless of Size" Criteria)

Regardless of score, an entity is automatically classified as **Tier 1** if:

1. **Sole provider** of an essential health service in a geographic area
2. Operates a **national-level** health information system
3. Operates **emergency ambulance dispatch** or **air ambulance** services
4. Operates **blood or organ allocation** services at national/regional level
5. Operates national/regional **infectious disease surveillance**
6. Explicitly designated by competent authority as **CII**

Part 4: System-Level Metrics

4.1 Critical Health Information Systems (Global Consensus)

The following systems are prioritized across **80%+ of jurisdictions**:

System Category	Criticality Rationale	Tier
Emergency Dispatch (CAD)	Immediate life-safety impact	1

System Category	Criticality Rationale	Tier
Hospital EMR/EHR (ICU/ED settings)	Direct patient care continuity	1
ICU Monitoring Systems	Real-time life support	1
Blood Bank/Transfusion	Immediate clinical dependency	1
Disease Surveillance	Epidemic response capability	1
National EHR/HIE	Systemic healthcare function	1
Operating Theatre Management	Surgical care continuity	1-2
Pharmacy Management	Medication safety	1-2
LIMS (Laboratory)	Diagnostic capability	2
RIS/PACS (Radiology)	Diagnostic capability	2
Hospital ADT/PAS	Administrative continuity	2
ePrescribing	Medication management	2
Immunization Registries	Public health function	2
Organ Transplant Allocation	Life-critical matching	1

4.2 System Criticality Scoring

Factor	Assessment Question	Score
Availability Impact	Service unavailable: life-threatening within 4 hours?	0-10
Integrity Impact	Data corruption: direct patient harm possible?	0-10
Confidentiality Impact	Breach: significant personal health data exposure?	0-10
Substitutability	Manual workaround available?	0-10
Recovery Time	RTO > 24 hours = critical	0-10

Total: 50 points maximum

Score	System Tier
≥35	Tier 1 System
20–34	Tier 2 System
<20	Tier 3 System

Part 5: Incident Impact Thresholds

5.1 UK-Style Quantitative Thresholds (Most Explicit Globally)

Impact Category	Threshold	Tier Applicability
Excess fatalities	>0	All tiers
Potential clinical harm	>50 patients at risk	Tier 1, 2

Impact Category	Threshold	Tier Applicability
ED closure/diversion	>3 hours (major trauma center)	Tier 1
ED closure/diversion	>24 hours (other hospitals)	Tier 2
Outpatient appointments cancelled	>1,500	Tier 1, 2
Inpatient episodes cancelled	>250	Tier 1, 2
Emergency call-taking unavailable	>3 hours	Tier 1
Data breach	>30,000 records	All tiers

5.2 Reporting Timelines (Global Convergence)

Reporting Stage	Standard	Tier 1	Tier 2	Tier 3
Early Warning	12–24 hours	12h	24h	N/A
Detailed Notification	48–72 hours	48h	72h	72h
Final Report	14–30 days	14d	30d	30d
Ransom Payment	24 hours	24h	24h	24h

Part 6: Composite Grading Framework

6.1 Final Classification Matrix

```
ENTITY CLASSIFICATION = f(Entity Score, System Criticality, Function Type)
```

```
              ┌──────────────────────────────────────────────────┐
              │                   FUNCTION TYPE                    │
              ├──────────────┬───────────────┬───────────────────┤
              │ Life–Safety  │  Diagnostic   │  Administrative   │
        ┌─────┼──────────────┼───────────────┼───────────────────┤
        │ Score ≥60 │ TIER 1 │    TIER 1     │      TIER 2       │
ENTITY  ├──────────────┼──────────────┼───────────────┼──────────┤
SCORE   │ Score 30–59│ TIER 1  │    TIER 2     │      TIER 2       │
        ├──────────────┼──────────────┼───────────────┼──────────┤
        │ Score <30 │ TIER 2  │    TIER 2     │      TIER 3       │
        └─────┴──────────────┴───────────────┴───────────────────┘
```

6.2 Obligations by Tier

Obligation	Tier 1	Tier 2	Tier 3
Risk Management Plan	Required	Required	Recommended
Security Officer (CISO)	Required	Required	Optional
Annual Risk Assessment	Required	Required	Recommended
Security Audit	Annual	Biennial	Self-assessment

Obligation	Tier 1	Tier 2	Tier 3
Incident Reporting	12h/48h mandatory	24h/72h mandatory	Voluntary
Cyber Exercise Participation	Mandatory	Encouraged	Voluntary
Supply Chain Security	Required	Required	Recommended
24/7 Monitoring	Required	Recommended	Optional
Business Continuity Plan	Required	Required	Recommended
Regulatory Supervision	Ex-ante	Ex-post	Self-regulated

6.3 Penalty Framework (Proportionate)

Tier	Maximum Administrative Fine	Basis
Tier 1	€10M or 2% global turnover	EU NIS2 model
Tier 2	€7M or 1.4% global turnover	EU NIS2 model
Tier 3	Warning → Compliance order	Graduated

Part 7: Implementation Guidance

7.1 Self-Assessment Questionnaire

Entities should complete the following to determine preliminary tier classification:

Question	Yes Score	No Score
Do you operate an ICU?	+25	0
Do you provide emergency ambulance dispatch?	+25	0
Do you operate blood/organ allocation services?	+20	0
Do you have ≥30,000 inpatient cases/year?	+30	0
Are you the sole provider of essential services in your area?	+10	0
Do you operate a national/regional disease surveillance system?	+20	0
Do you have ≥50 employees?	+10	0
Do other health systems depend on your systems?	+8	0

Preliminary Classification: - Score ≥60 → Likely Tier 1 - Score 30–59 → Likely Tier 2 - Score <30 → Likely Tier 3

7.2 Regulatory Review Process

1. **Self-Assessment** → Entity completes questionnaire and submits to regulator
2. **Validation** → Regulator reviews against national health data
3. **Designation** → Entity receives written notification of tier classification
4. **Appeals** → 30-day window to contest classification
5. **Periodic Review** → Classification reviewed every 2 years (EU NIS2 model)

7.3 Transition Timeline

Phase	Timeline	Activity
Phase 1	Months 1-3	Self-assessment by entities
Phase 2	Months 4-6	Regulatory validation and designation
Phase 3	Months 7-12	Compliance planning and gap analysis
Phase 4	Months 13-18	Full compliance (Tier 1 first)
Phase 5	Months 19-24	Full compliance (all tiers)

Part 8: Reference Jurisdictions for Each Component

Framework Component	Primary Reference	Secondary Reference
Quantitative thresholds	Germany (BSI-KritisV)	Australia (SOCI Act)
Three-tier structure	EU NIS2, Israel	Hong Kong
Incident reporting timelines	Hong Kong, Norway	EU NIS2
Impact thresholds	UK (DHSC CAF)	—
"Regardless of size" triggers	EU NIS2	Singapore
System-level designation	Singapore (CII)	Hong Kong
Public criteria/confidential lists	Most jurisdictions	South Korea (exception: public)
Proportionate penalties	EU NIS2	Hong Kong
Registration obligation	Germany (NIS2)	Taiwan
Periodic review	EU NIS2 (2-year)	UK

Part 9: Developing Country Adaptations

[!IMPORTANT] The thresholds derived from European, North American, and Australian frameworks (Parts 1-8) are calibrated for **developed healthcare systems** with high IT maturity, abundant regulatory capacity, and relatively uniform digital infrastructure. **Direct application to developing countries may be problematic** and requires significant adaptation.

9.1 Why Developed-Country Thresholds Are Inappropriate

Factor	Developed Country Context	Developing Country Reality
Case volume	30,000 inpatient cases = mid-size hospital	30,000 cases may be a **major tertiary center**
ICU availability	Most hospitals have ICUs	ICU availability concentrated in metros; many districts have **zero ICU beds**
Employee count	50 employees = small clinic	50 employees may be a **district hospital**
Digital maturity	EHR penetration >80%	EHR penetration may be <20% in public sector
Regulatory capacity	Dedicated cyber agencies with health expertise	Nascent regulatory capacity; limited health-cyber specialists
Connectivity	Ubiquitous broadband	Intermittent connectivity in rural areas; offline-first systems critical
Health system structure	Insurance-based or tax-funded universal	Mixed public-private; large informal sector

9.2 Adapted Threshold Framework for Developing Countries

A. Inpatient Case Volume (Adjusted)

Tier	Developed Country Threshold	Developing Country Threshold	Rationale
Tier 1	≥30,000 cases/year	≥10,000 cases/year	Lower threshold captures district/tertiary hospitals
Tier 2	5,000–29,999	2,000–9,999	Community and sub-district hospitals
Tier 3	<5,000	<2,000	PHCs and small facilities

B. Bed Count Alternative (Where Case Data Unavailable)

Tier	Developed Country	Developing Country (e.g., India)
Tier 1	≥500 beds	≥200 beds OR District Hospital status
Tier 2	100–499 beds	50–199 beds OR Sub-District Hospital
Tier 3	<100 beds	<50 beds OR PHC/CHC

C. Employee Count (Adjusted)

Tier	EU NIS2 Threshold	Developing Country Threshold
Tier 1	≥250 employees	≥100 employees
Tier 2	50–249 employees	25–99 employees
Tier 3	<50 employees	<25 employees

9.3 India-Specific Critical Information Systems

Beyond the globally-recognized systems, **India has unique national digital health systems** that warrant CII consideration:

System	Description	Criticality	Suggested Tier
Ayushman Bharat Digital Mission (ABDM)	National digital health ID and ecosystem	National HIE equivalent	Tier 1
PM-JAY (Pradhan Mantri Jan Arogya Yojana)	National health insurance platform for 500M+ beneficiaries	Financial access to healthcare	Tier 1
CoWIN	COVID vaccination platform; adaptable for routine immunization	National immunization system	Tier 1
eVIN (Electronic Vaccine Intelligence Network)	Cold chain and vaccine inventory management	Supply chain criticality	Tier 1-2
IHIP (Integrated Health Information Platform)	Disease surveillance and outbreak response	Epidemic response	Tier 1
NIKSHAY	TB surveillance and treatment tracking	Public health surveillance	Tier 1-2
RCH Portal (Reproductive & Child Health)	Maternal and child health tracking	Population health	Tier 2
HMIS/eHospital	Hospital management for central/state government hospitals	Hospital operations	Tier 2

System	Description	Criticality	Suggested Tier
NIC infrastructure for emergency services	112 ERSS (Emergency Response Support System)	Emergency dispatch	Tier 1
National Blood Transfusion Council systems	Blood bank management	Blood supply chain	Tier 1-2

9.4 Geographic and Accessibility Criteria

In developing countries, **geographic accessibility** is a more relevant criticality factor than pure scale:

Criterion	Application	Weight
Sole provider in district	Only hospital with surgical/obstetric capability in district	Automatic Tier 1
Distance to next facility	Nearest equivalent facility >50km away	+15 points
Population served without alternative	Serves >100,000 population as primary referral	+15 points
Border/remote area	Located in border districts, islands, or hill regions with limited connectivity	+10 points
Aspirational district	Located in government-designated "aspirational district"	+10 points

India-Specific Geographic Triggers   An entity should be automatically classified as **Tier 1** if:

1. **District Hospital** — Only referral hospital in the district
2. **FRU (First Referral Unit)** — Only facility with C-section/blood transfusion capability in the block/sub-district
3. **State reference laboratory** — Only accredited reference lab in the state
4. **Blood bank (standalone)** — Only licensed blood bank in the district
5. **Major Government Medical College Hospital** — Apex referral and training institution

9.5 Tiered Public Health System Considerations

India's **tiered public health infrastructure** requires adapted tier mapping:

Health Facility Type	Typical Characteristics	Suggested CII Tier
AIIMS / National Institutes	Apex tertiary + research; 1,000+ beds	Tier 1

Health Facility Type	Typical Characteristics	Suggested CII Tier
State/Central Government Medical College Hospitals	Major tertiary; 500-1,500 beds	Tier 1
District Hospital (DH)	District headquarters; 100-500 beds; surgery/obstetrics	Tier 1 (if sole in district)
Sub-District Hospital (SDH)	Taluk/sub-district; 30-100 beds	Tier 2
Community Health Centre (CHC)	Block level; 30 beds; FRU function	Tier 2 (if sole FRU in block)
Primary Health Centre (PHC)	Primary care; 6 beds; limited digital systems	Tier 3
Health & Wellness Centre (HWC)	Sub-centre upgrade; ASHA coordination	Tier 3
Major Private Corporate Hospitals	200+ beds; multi-specialty; extensive IT	Tier 1-2 (based on scale/function)

9.6 Digital Maturity Considerations

Factor	Developed Country Assumption	Developing Country Reality	Adaptation
EHR adoption	Universal or near-universal	Variable; paper-based common	Prioritize facilities with digital systems for CII scope
Internet connectivity	Always-on broadband	Intermittent; mobile-dependent	**Offline-capable systems** as critical; data sync mechanisms
IT staffing	Dedicated IT/security teams	Often shared/outsourced; limited capacity	**Shared services** (state-level SOC) as Tier 1 system
Cloud vs on-premise	Cloud-first / hybrid	On-premise or central data centers	**State Data Centers (SDCs)** hosting health systems as Tier 1

Factor	Developed Country Assumption	Developing Country Reality	Adaptation
Supply chain visibility	Integrated vendor management	Fragmented; informal procurement	Lower emphasis on third-party risk scoring initially

9.7 Regulatory and Compliance Capacity

Challenge	Developed-Country Approach	Developing-Country Adaptation
Limited regulators	Sector-specific competent authorities	**Single nodal agency** with health ministry support
Audit capacity	Annual third-party audits	**Phased approach**: Tier 1 first; self-assessment for Tier 3
Incident reporting	Real-time portals; dedicated CERT	**Simplified reporting**: SMS/email fallback; longer initial timelines
Penalties	€10M+ fines	**Proportionate**: Compliance orders first; modest fines scaled to public sector budgets
Technical guidance	Sector-specific security standards	**Adopt/adapt** existing standards (ISO 27799, NIST Healthcare) with local context

9.8 Adapted Incident Reporting Timelines

Reporting Stage	Developed Country	Developing Country (Initial Phase)	Rationale
Early Warning	12–24 hours	24–48 hours	Account for connectivity and capacity limitations
Detailed Notification	48–72 hours	72–96 hours	More time for investigation in resource-limited settings
Final Report	14–30 days	30–45 days	Extended analysis period

Reporting Stage	Developed Country	Developing Country (Initial Phase)	Rationale
Ransom Payment	24 hours	24 hours	Keep consistent for law enforcement coordination

9.9 India-Specific "Regardless of Size" Triggers

Regardless of scale, an entity should be **automatically Tier 1** in India if it:

1. Operates **ABDM (Ayushman Bharat Digital Mission)** infrastructure at national/state level
2. Operates **PM-JAY** transaction processing or beneficiary management systems
3. Is the **sole government hospital** in a district
4. Operates **112 ERSS** (National Emergency Number) dispatch for any state
5. Operates **state-level integrated disease surveillance** (IHIP)
6. Is a **national or regional reference laboratory** (NCDC, NIV, ICMR labs)
7. Operates **state blood bank council** or regional blood transfusion center
8. Is a **State Data Center** hosting health applications
9. Provides **telemedicine hub services** for remote/tribal areas (e.g., eSanjeevani hubs)
10. Operates **cold chain management systems** (eVIN) at state level

9.10 Developing Country Scoring Adjustments

Adjusted Scoring Matrix for Developing Countries

Domain	Criterion	Points (Developed)	Points (Developing)
A. Scale			
	≥10,000 inpatient cases/year	—	30
	5,000–9,999 cases/year	—	20
	2,000–4,999 cases/year	—	10
B. Public System Role			
	District Hospital (sole in district)	—	25
	FRU (sole in block)	—	20
	CHC/PHC digitized	—	5
C. Geographic Criticality			
	Sole provider >50km radius	—	20
	Aspirational/border district	—	10
	Remote/tribal area	—	10
D. National Program Integration			
	Hosts ABDM/PM-JAY systems	—	25
	State disease surveillance node	—	20
	eVIN/immunization registry	—	15

9.11 Phased Implementation Approach

Given capacity constraints, developing countries should adopt a **phased rollout**:

Phase	Timeline	Scope	Focus
Phase 1	Year 1	National systems only	ABDM, PM-JAY, 112 ERSS, national surveillance, State Data Centers
Phase 2	Year 2	Tier 1 entities (national + major tertiary)	AIIMS, GMCHs, major private chains, state blood banks
Phase 3	Year 3-4	Tier 2 entities (district level)	District hospitals, state reference labs, regional facilities
Phase 4	Year 5+	Tier 3 entities (voluntary)	PHCs, CHCs, small private hospitals

9.12 Capacity Building Requirements

Requirement	Developed Country	Developing Country Approach
Sector-specific guidance	Published standards (B3S, CAF)	**Develop simplified health CII security baseline**
Training	Commercial certifications	**Subsidized/free government training programs**
Shared services	Commercial MSPs	**State-level Security Operations Centers (SOCs)** for public health facilities
Incident response	Sector CERTs	**National Health-CERT** with state nodes
Technical assistance	Market-driven consulting	**Government technical support units** for compliance assistance

9.13 Developing Country Case Studies

The following jurisdictions provide relevant models for adapting CII frameworks to developing country contexts:

A. China: Multi-Level Protection Scheme (MLPS) for Healthcare **Key Features:** - **Five-tier grading system** (Levels 1-5) applied to all network information systems - **Explicit health-sector guidance** (2011 NHC directive) specifying which systems are "≥ Level 3" - **Party-state designation authority** rather than purely market-based self-assessment

Systems Explicitly Designated Level 3+ (Health Sector):

System Type	Level	Scope
Cross-province national networked systems (infectious disease reporting, health statistics)	≥3	National
National/provincial/municipal health information platforms	≥3	National/Provincial
Core business information systems of **Class III Grade A hospitals** (三级甲等医院)	≥3	Major tertiary hospitals
New Rural Cooperative Medical Scheme (NRCMS) systems	≥3	National
Health supervision and maternal & child health registries	≥3	National

Relevance for India: - China's "Class III Grade A" hospital threshold is conceptually similar to India's **AIIMS/major government medical college** tier - The MLPS **annual evaluation requirement** for Level 3+ systems could inform India's audit approach - Focus on **public health surveillance systems** as automatic high-tier matches India's IHIP context

---

B. Thailand: Public Health as CII Sector   Key Features: - **Cybersecurity Act B.E. 2562 (2019)** explicitly includes **"Public Health"** as a CII sector (Section 49) - **Committee-based designation** (case-by-case review by NCSC Committee) - **Three cyber threat levels** (non-critical / critical / crisis) with "public health" explicitly referenced in "critical level" definition - **September 2025 CII List Revision** updated health sector designations

Designation Mechanism:

Element	Thailand Approach	Applicability
Sector trigger	"Public health" listed in Section 49 aspects	Qualitative, broad
Designation process	Committee notification → case-by-case review → Government Gazette publication	Administrative discretion
No numeric thresholds	Qualitative ("maintaining national security, public security, national economic security")	Flexible for diverse health system
Annual assessment	Risk assessment + examination at least once per year	Realistic for developing context
Penalty	฿200,000 fine for non-reporting (modest by global standards)	Proportionate

Relevance for India: - Thailand's **qualitative designation** with committee discretion suits contexts where quantitative data is unreliable - **Annual assessment** (not biennial) is achievable for high-tier facilities - **Modest penalties** more appropriate than EU-style €10M fines for public-sector hospitals

---

C. Malaysia: National Critical Information Infrastructure (NCII) **Key Features:** - **NACSA (National Cyber Security Agency)** lists **"Healthcare Services"** as an NCII sector - **Sector-based approach** with sector leads responsible for designation - Part of broader **11-sector NCII framework**

Model Elements:

Element	Malaysia Approach
Governing body	NACSA (centralized coordination)
Sector implementation	Ministry of Health as sector lead
Scope	Hospitals, clinics, public health agencies
Reporting	Incident reporting to sector regulator → NACSA

Relevance for India: - Malaysia's **sector lead model** (health ministry coordination with central cyber agency) aligns with India's potential MoHFW + CERT-In + NCIIPC structure - NACSA's role as **coordinating body** (not sole designator) mirrors India's federated model with state health departments

---

D. Indonesia: Vital Information Infrastructure (Perpres 82/2022) **Key Features:** - **Presidential Regulation 82/2022** establishes Vital Information Infrastructure protection - **"Sektor Kesehatan" (Health Sector)** explicitly listed as strategic sector - **BSSN (National Cyber and Crypto Agency)** as coordinating regulator

Framework Structure:

Element	Indonesia Approach
Legal basis	Presidential Regulation (Perpres) — fast executive action
Sector classification	Health listed among strategic sectors
Designation authority	Sector ministry with BSSN coordination
Implementation	Still developing detailed health-sector guidelines

Relevance for India: - Indonesia's use of **executive regulation** (Perpres) rather than primary legislation enables faster implementation - Could inform India's approach via **IT Act rules** or **DPDP Act rules** rather than new legislation - Both countries share **archipelago/large-geography** challenges requiring offline-first system considerations

---

E. Ghana: African Model for Health CII **Key Features:** - **Cyber Security Authority (CSA) directive** explicitly lists **"Health"** as a CII sector - Part of **national CII protection framework** under Cybersecurity Act 2020 - Relatively early adopter in Sub-Saharan Africa

Relevance for India: - Demonstrates that **even resource-limited contexts** can establish explicit health CII frameworks - Ghana's approach emphasizes **sector listing first, detailed thresholds later** — incremental model

---

F. Kazakhstan / Kyrgyz Republic: Central Asian Models **Key Features:** - Both jurisdictions **explicitly include "healthcare"** in their CII/CIIC definitions - **Legal text definitions** rather than detailed implementation guidance - Reflects **post-Soviet legal tradition** of broad framework laws

Country	Definition	Source
Kazakhstan	"Critical information and communication infrastructure" explicitly includes **healthcare**	Adilet LIS CIIC Rules
Kyrgyz Republic	"Critical information infrastructure" includes the field of **healthcare**	Regulation for Information Protection in SIS

Relevance for India: - Shows that **explicit sector listing in law** is foundational — India could do this via IT Act amendment or DPDP rules - Central Asian models are also adapting **Russian-style graduated protection** (similar to China's MLPS)

9.14 Comparative Summary: Developing Country Models

Feature	China	Thailand	Malaysia	Indonesia	India (Proposed)
Sector explicitly listed	☐ (MLPS, CII Reg)	☐ (Section 49)	☐ (NCII)	☐ (Perpres 82/2022)	☐ (Recommend)
Tiering system	5 levels	3 threat levels	Binary	Binary	3 tiers
Quantitative thresholds	No (Class III-A qualitative)	No	No	No	Yes (adapted)
Hospital tier explicit	Class III-A	No	No	No	Yes (AIIMS/DH/PHC)
National systems separate	Yes (Level 3+)	Implicit	Implicit	Implicit	Yes (ABDM, PM-JAY)
Geographic factors	No	No	No	No	Yes (sole provider)
Audit frequency	Annual (Level 3+)	Annual	Not specified	Not specified	Annual (T1) / Biennial (T2)
Penalties	Administrative sanctions	฿200K fine	Not specified	Not specified	Proportionate

Feature	China	Thailand	Malaysia	Indonesia	India (Proposed)
Legal instrument	Law + State Council Reg	Cybersecurity Act	Agency directive	Presidential Reg	IT Act rules / new law

9.15 Recommended Approach for India

Based on global developing country models, the recommended approach for India:

1. **Explicit sector listing**: Amend IT Act rules or issue executive notification explicitly designating "Healthcare" as CII sector under existing NCIIPC framework
2. **Tiered designation with geographic factors**: Adopt 3-tier model with:
   - **Tier 1**: National digital systems + AIIMS/GMCHs + sole district providers
   - **Tier 2**: District hospitals + reference labs + major private chains
   - **Tier 3**: PHCs/CHCs (voluntary/self-regulated)
3. **Qualitative + quantitative hybrid**: Use adapted quantitative thresholds (10,000 cases/year, 200 beds) with qualitative triggers (sole provider, geographic remoteness)
4. **Committee-based designation** (Thailand model): Health-CII Designation Committee with MoHFW, MeitY, NCIIPC, and CERT-In representation
5. **Phased implementation** (China model):
   - Year 1: National systems (ABDM, PM-JAY, 112 ERSS)
   - Year 2: Tier 1 facilities
   - Year 3-4: Tier 2 facilities
6. **Proportionate obligations**:
   - Tier 1: Annual audits, 24-48h reporting, mandatory BCP
   - Tier 2: Biennial audits, 72-96h reporting
   - Tier 3: Self-assessment, voluntary reporting
7. **Shared services model**: State-level SOCs for public health facilities (leveraging NIC/state IT infrastructure)
8. **Health-CERT**: Establish sectoral CERT under MoHFW with CERT-In coordination (similar to sectoral CERTs in banking/power)

Conclusion

This metrics and grading framework provides a **structured, evidence-based approach** for classifying health sector entities as Critical Information Infrastructure. Key design principles include:

1. **Hybrid criteria**: Combines quantitative thresholds with qualitative safety-net triggers
2. **Proportionality**: Three-tier structure aligns obligations with criticality
3. **Transparency**: Clear criteria enable self-assessment
4. **Adaptability**: Framework accommodates diverse health system contexts
5. **Global alignment**: Harmonized with emerging international standards

The framework should be adapted to national context, with particular attention to: - Local health system structure and governance - Existing regulatory frameworks - Data availability for quantitative

---

References

This framework synthesizes criteria from the 17 jurisdictions analyzed in this study:

1. USA (CISA/HPH Sector)
2. Australia (SOCI Act 2018)
3. European Union (NIS2 Directive)
4. Canada (National CI Strategy)
5. United Kingdom (NIS Regulations / CAF)
6. Germany (BSI-KritisV / NIS2UmsuCG)
7. Singapore (Cybersecurity Act)
8. New Zealand (HISO 10029 / NVA)
9. Japan (CIP Policy)
10. China (Cybersecurity Law / MLPS)
11. South Korea (CIIC Act)
12. France (OIV/SAIV/SIIV)
13. Norway (Digital Security Act)
14. Switzerland (ISG/CSV)
15. Taiwan (CSMA)
16. Thailand (Cybersecurity Act)
17. Hong Kong (PCICSO)

CII Case Studies: Healthcare Delivery Facilities

This chapter presents case studies for **healthcare delivery facilities** including hospitals, medical colleges, community health centres, and telemedicine services.

Case Study 1: Metro General Hospital

Entity Profile

Attribute	Details
Name	Metro General Hospital
Type	Government tertiary teaching hospital
Location	State capital city (population 5 million)
Beds	1,200
Annual inpatient cases	45,000
Employees	3,500
Key departments	ICU (50 beds), Emergency, Trauma Centre, Cardiac Surgery, Organ Transplant
Digital systems	Integrated HIS, EMR, PACS, LIS, Blood Bank Management
Connectivity	24/7 broadband; connected to national health exchange

CII Classification Assessment

Scoring (Developed Country Framework)

Domain	Criterion	Points Scored
A. Scale	≥30,000 cases/year	30
B. Capability	General ICU present	25
C. Functions	Blood bank/transfusion + Organ allocation	20
D. Uniqueness	Alternative providers available (metro area)	0
E. Dependencies	Other regional facilities depend on transplant services	8
TOTAL		**83**

Scoring (Developing Country Framework - Adapted)

Domain	Criterion	Points Scored
A. Scale	≥10,000 cases/year	30
B. Public System Role	Major Government Medical College	25
C. Geographic Criticality	Metro (not sole provider)	0
D. National Program Integration	Connected to national HIE	15
TOTAL		**70**

Classification Result

Framework	Score	Tier	Rationale
Developed Country	83	**Tier 1 (Essential)**	Exceeds 60-point threshold; ICU + transplant capability
Developing Country	70	**Tier 1 (Essential)**	Major teaching hospital; national program integration

Applicable Obligations

- Annual security audit (third-party)
- 24-48 hour incident reporting
- Dedicated CISO required
- Mandatory business continuity plan
- Participation in cyber drills
- 24/7 security monitoring

Case Study 2: Rural District Hospital - Greenfield DH

Entity Profile

Attribute	Details
Name	Greenfield District Hospital
Type	Government district hospital
Location	Rural district headquarters (district population 1.2 million)
Beds	150
Annual inpatient cases	8,000
Employees	280
Key departments	General surgery, Obstetrics, Emergency, No ICU
Digital systems	Basic HIS, connected to state disease surveillance
Connectivity	Intermittent broadband; mobile backup

Attribute	Details
Special status	**Only hospital with surgical capability in the district**

CII Classification Assessment

Scoring (Developed Country Framework)

Domain	Criterion	Points Scored
A. Scale	5,000–14,999 cases/year	10
B. Capability	Emergency department only (no ICU)	10
C. Functions	None of the critical functions listed	0
D. Uniqueness	Sole provider in region	10
E. Dependencies	Limited external dependencies	3
TOTAL		**33**

Scoring (Developing Country Framework - Adapted)

Domain	Criterion	Points Scored
A. Scale	5,000–9,999 cases/year	20
B. Public System Role	District Hospital (sole in district)	25
C. Geographic Criticality	Sole provider >50km radius	20
D. National Program Integration	State disease surveillance node	10
TOTAL		**75**

Classification Result

Framework	Score	Tier	Rationale
Developed Country	33	**Tier 2 (Important)**	Above 30 threshold; sole provider adds weight
Developing Country	75	**Tier 1 (Essential)**	**Automatic Tier 1 trigger:** Sole district hospital

[!IMPORTANT] This case illustrates why developing country adaptations are critical. Under developed-country thresholds, this hospital would be Tier 2. However, as the **sole surgical/obstetric facility for 1.2 million people**, it merits Tier 1 designation in the developing country context.

Applicable Obligations (Developing Country Tier 1)

- Annual security audit (may be state-supported)
- 24-48 hour incident reporting
- Security focal point required (may share with district administration)
- Business continuity plan with manual fallback procedures
- State SOC integration (shared services model)

Case Study 3: Private Hospital Chain - HealthFirst Network

Entity Profile

Attribute	Details
Name	HealthFirst Hospital Network
Type	Private corporate hospital chain
Coverage	15 hospitals across 8 states
Total beds	4,500 (average 300 per hospital)
Annual inpatient cases	180,000 (network-wide)
Employees	12,000
Key features	ICU in all facilities; 3 hospitals with cardiac surgery
Digital systems	Centralized cloud EHR; unified patient portal
Market position	Second-largest private chain in the country

CII Classification Assessment

Entity-Level vs System-Level Analysis

Analysis Level	Scope	Approach
Entity-level (network)	Entire chain as single entity	Aggregate scoring
System-level	Centralized EHR platform	System criticality assessment
Facility-level	Each hospital individually	Facility-by-facility scoring

Network-Level Scoring (Developing Country)

Domain	Criterion	Points Scored
A. Scale	≥10,000 cases/year (network: 180,000)	30
B. Capability	ICU present in all facilities	25

Domain	Criterion	Points Scored
C. Geographic Criticality	Multi-state presence; alternative providers in most locations	5
D. National Program Integration	PM-JAY empaneled; national HIE connected	20
TOTAL		**80**

System-Level Assessment: Centralized EHR Platform

Factor	Assessment	Score
Availability Impact	Outage affects 180,000 patients/year across 15 hospitals	10
Integrity Impact	Data corruption could affect treatment decisions	9
Confidentiality Impact	Millions of patient records at risk	9
Substitutability	Paper fallback possible but severely impacts operations	7
Recovery Time	RTO estimated 48+ hours for full restoration	9
TOTAL		**44**

Classification Result

Level	Score	Tier	Rationale
Network (entity)	80	**Tier 1**	Scale + capability + national program integration
Centralized EHR (system)	44	**Tier 1 System**	High criticality across all factors
Individual hospitals	Varies	**Tier 1 or 2**	Based on local sole-provider status

Applicable Obligations

Network-level: - Dedicated Group CISO required - Annual third-party audit of centralized systems - 24-hour incident reporting for centralized platform incidents - Participation in national cyber drills - Supply chain security assessment for cloud vendors

Facility-level: - Site-level security focal points - Local business continuity plans - Integration with network SOC

Case Study 4: Community Health Centre - Riverside CHC

Entity Profile

Attribute	Details
Name	Riverside Community Health Centre
Type	Government block-level CHC
Location	Rural block (block population 120,000)
Beds	30
Annual inpatient cases	1,200
Employees	45
Key departments	General OPD, Labor room, No surgery, No ICU
Digital systems	RCH portal access; immunization tracking
Connectivity	Mobile data; intermittent connectivity
Special status	Not designated as First Referral Unit (FRU)

CII Classification Assessment

Scoring (Developing Country Framework)

Domain	Criterion	Points Scored
A. Scale	<2,000 cases/year	5
B. Public System Role	CHC (not FRU, not sole in block)	5
C. Geographic Criticality	District hospital 35km away	5
D. National Program Integration	RCH portal access	5
TOTAL		**20**

Classification Result

Framework	Score	Tier	Rationale
Developing Country	20	**Tier 3 (Baseline)**	Small scale; not sole provider; limited digital footprint

Applicable Obligations (Tier 3)

- Self-assessment recommended
- Voluntary incident reporting
- Basic cyber hygiene guidance
- May benefit from state-level shared services (SOC, backup)
- Not subject to mandatory audits or reporting timelines

Case Study 5: Telemedicine Hub - "Sehat Setu"

Entity Profile

Attribute	Details
Name	Sehat Setu Regional Telemedicine Hub
Type	Government telemedicine hub serving remote/tribal areas
Coverage	3 remote districts; 200 spoke locations
Functions	Video consultations; specialist referrals; prescription support
Consultations	150,000 per year
Employees	35
Population served	2.5 million (primarily tribal, remote)
Special status	Only specialist access for tribal blocks

CII Classification Assessment

Scoring (Developing Country Framework)

Domain	Criterion	Points Scored
A. Scale	Not a hospital (consultations-based)	10
B. Public System Role	Government telemedicine hub	15
C. Geographic Criticality	Sole specialist access for remote population	20
D. Functions	Telemedicine hub for tribal/remote areas	15
TOTAL		**60**

Classification Result

Framework	Score	Tier	Rationale
Developing Country	60	**Tier 1 (Essential)**	Threshold met; sole specialist access for underserved population

[!NOTE] This case demonstrates how **telemedicine hubs serving remote populations** can qualify as Tier 1 despite modest scale, because they represent the **only access point** for specialist care.

Applicable Obligations

• Security focal point

- 24-48 hour incident reporting
- Business continuity: Backup connectivity; manual referral protocols
- Annual audit (may be combined with state ICT audit)
- Data protection: Patient consultation confidentiality

Case Study 6: Medical College Research Institution - "Lakshmi Devi Medical College"

Entity Profile

Attribute	Details
Name	Lakshmi Devi Medical College & Research Institute
Type	Government medical college with attached teaching hospital
Location	State capital city
Beds	1,500 (attached hospital)
Annual admissions	MBBS: 250; PG: 150; Super-specialty: 50
Research programs	45 active research projects; 12 clinical trials
Research funding	₹50 crore active grants (national and international)
Key systems	Hospital Information System (HIS), Clinical Trial Management System (CTMS), Electronic Lab Notebook (ELN), Research Data Repository, Student Information System
Data holdings	25 years of patient records; 200,000+ research subjects data
Integrations	Connected to national clinical trial registry; multiple international research collaborations
Special consideration	**Dual role: clinical care + research training pipeline**

CII Classification Assessment

Dual Assessment: Clinical vs Research Functions

Function	Criticality Basis
Clinical care	Major tertiary hospital with ICU, trauma, specialty services
Medical education	Trains future healthcare workforce; pipeline criticality
Research	Clinical trials, longitudinal studies, collaborative research data

Function	Criticality Basis
Research IP	Proprietary research findings, unpublished data

Scoring (Developing Country Framework)

Domain	Criterion	Points Scored
A. Clinical Scale	1,500 beds; major tertiary hospital	30
B. Capability	ICU, emergency, tertiary specialty services	25
C. Research Function	45 active projects; clinical trial data	15
D. Training Pipeline	450 trainees/year; workforce development	10
TOTAL		**80**

Classification Result

Framework	Score	Tier	Rationale
Developing Country	80	**Tier 1 (Essential)**	Major tertiary hospital + research institution + training function

[!NOTE] Medical colleges have **triple criticality**: clinical care, research data, and workforce training. A cyber incident affecting a medical college simultaneously impacts patient care, ongoing research, and future healthcare capacity.

Applicable Obligations

Clinical side: - All Tier 1 hospital obligations (CISO, audit, incident reporting, BCP)

Research side: - Research data protection controls (ELN, CTMS, repositories) - Clinical trial data integrity monitoring - International collaboration data transfer controls - Research ethics committee security awareness

Education side: - Student data protection - Examination system security - Training continuity planning

---

Summary: Healthcare Delivery Classification

Case Study	Entity Type	Score	Tier
Metro General Hospital	Tertiary teaching	70	**Tier 1**
Greenfield District Hospital	District hospital (sole)	75	**Tier 1** (auto)
HealthFirst Network	Private chain	80	**Tier 1**
Riverside CHC	Community health centre	20	**Tier 3**
Sehat Setu Telemedicine	Remote telemedicine hub	60	**Tier 1**
Lakshmi Devi Medical College	Medical college + research	80	**Tier 1**

Key Insights

1. **Geographic factors outweigh scale**: Sole district hospitals are Tier 1 regardless of size
2. **Private chains can be CII**: Large networks with centralized systems warrant high classification
3. **Telemedicine criticality**: Access-based criticality applies to underserved population hubs
4. **Medical colleges have compound criticality**: Clinical + research + training functions multiply risk
5. **Tier 3 facilities benefit from shared services**: Even unclassified facilities need security resources

CII Classification Case Studies: Overview and Index

This document provides an **overview and index** for the illustrative case studies demonstrating how to apply the CII Metrics and Grading Framework to health sector entities. All names, locations, and specific details are **fictional placeholders** designed to represent realistic scenarios.

Case Study Chapters

The case studies are organized into domain-specific chapters:

Chapter	Domain	Case Studies	File
61	Healthcare Delivery Facilities	6	61 - Case Studies - Healthcare Delivery.md
62	Digital Health Platforms	4	62 - Case Studies - Digital Health Platforms.md
63	Diagnostics, Pharma & Biotech	4	63 - Case Studies - Diagnostics Pharma Biotech.md
64	Public Health Programs & Surveillance	5	64 - Case Studies - Public Health Programs.md
65	Registries, Biobanks & Blood Services	3	65 - Case Studies - Registries Biobanks Blood.md
Total		**22**	

Complete Case Study Index

Healthcare Delivery Facilities (Chapter 61)

#	Case Study Name	Entity Type	Score	Tier
1	Metro General Hospital	Tertiary teaching hospital	70	**Tier 1**
2	Greenfield District Hospital	District hospital (sole provider)	75	**Tier 1 (auto)**
3	HealthFirst Network	Private hospital chain (15 hospitals)	80	**Tier 1**
4	Riverside CHC	Community health centre	20	**Tier 3**
5	Sehat Setu	Telemedicine hub (remote areas)	60	**Tier 1**
6	Lakshmi Devi Medical College	Medical college + research	80	**Tier 1**

Digital Health Platforms (Chapter 62)

#	Case Study Name	Entity Type	Score	Tier
7	SwasthyaSetu	National digital health platform	Auto	**Tier 1 (auto)**
8	MyHealthVault	PHR/health data aggregator	70	**Tier 1**
9	SwasthyaMitra	State HMIS (500+ hospitals)	80	**Tier 1**
10	CareSync Enterprise	Multi-hospital HMIS (5 hospitals)	45	**Tier 2**

Diagnostics, Pharma & Biotech (Chapter 63)

#	Case Study Name	Entity Type	Score	Tier
11	DiagnoFirst Labs	Private diagnostic lab chain	60	**Tier 1**
12	GenomeIndia Labs	Genomic sequencing laboratory	85	**Tier 1**
13	BioShield Pharma	Vaccine manufacturer	90	**Tier 1 (auto)**
14	GeneSys BioTech	Biosimilar R&D company	70	**Tier 1**

Public Health Programs & Surveillance (Chapter 64)

#	Case Study Name	Entity Type	Score	Tier
15	SurveilHealth	National disease surveillance	85	**Tier 1** (auto)
16	TB-Mukt Bharat	National TB elimination program	80	**Tier 1** (auto)
17	Sankalp	National NCD program	75	**Tier 1**
18	DrishtiRaksha	National blindness control	60	**Tier 1**
19	Poshan Rakshak	National nutrition program	80	**Tier 1** (auto)

Registries, Biobanks & Blood Services (Chapter 65)

#	Case Study Name	Entity Type	Score	Tier
20	OncoWatch	National cancer registry	85	**Tier 1** (auto)
21	JeevanKosh	National biobank	85	**Tier 1**
22	Jeevan Raksha	State blood transfusion council	70	**Tier 1** (auto)

Overall Tier Distribution

Tier	Count	Percentage	Representative Entities
Tier 1	20	91%	National platforms, major hospitals, surveillance systems, manufacturers
Tier 2	1	4.5%	Regional HMIS (5 hospitals)
Tier 3	1	4.5%	Small CHC

[!NOTE] The high proportion of Tier 1 classifications reflects the **intentional selection of diverse critical entities** for illustration. In practice, most health sector entities (small clinics, standalone pharmacies, individual practitioners) would be Tier 3 or unclassified.

Key Insights Across All Case Studies

Healthcare Delivery

1. **Geographic factors outweigh scale in developing countries**: Sole district hospitals qualify for Tier 1 regardless of size

2. **Private chains can be CII**: Large networks with centralized systems warrant high classification
3. **Telemedicine hubs have access-based criticality**: Remote populations depend on these as sole specialist access points
4. **Medical colleges have triple criticality**: Clinical care + research + workforce training compound the risk

Digital Health Platforms

5. **National platforms are automatic Tier 1**: Any national-level health information system triggers automatic classification
6. **Data aggregation creates concentrated risk**: PHR platforms aggregating from thousands of sources have unique criticality
7. **HMIS scale determines tier**: 500+ facilities = Tier 1; 5 facilities = Tier 2

Diagnostics, Pharma & Biotech

8. **Major diagnostic chains are CII**: Laboratories with significant market share and surveillance roles qualify for Tier 1
9. **Genomic data has unique sovereignty implications**: Population genomics is a national asset requiring special protection
10. **Supply chain entities are CII**: Vaccine/pharma manufacturers with significant market share are Critical Infrastructure
11. **IP-based criticality is valid**: High-value biotech research IP warrants CII consideration for economic security

Public Health Programs & Surveillance

12. **National surveillance is foundational CII**: Pandemic preparedness depends on surveillance system integrity
13. **Disease control programs have supply chain dependencies**: TB drugs, IOL distribution, nutrition supplements are attack vectors
14. **NCD programs need longitudinal integrity**: Chronic disease tracking requires decade-long data protection
15. **Child health programs are life-critical**: Nutrition monitoring directly affects child mortality

Registries, Biobanks & Blood Services

16. **Disease registries support public health planning**: National registry data is irreplaceable
17. **Biobanks need hybrid security**: Physical sample integrity + cyber data protection are equally critical
18. **Blood services are life-critical**: Real-time coordination for emergency transfusions has immediate mortality implications

---

Using These Case Studies

For Policymakers

- Use case studies to **illustrate framework application** to stakeholders
- Adapt scoring criteria based on **local context and thresholds**
- Reference developing country adaptations for **proportionate implementation**

For Regulators

- Use as **templates for self-assessment questionnaires**
- Apply scoring methodology consistently across entities
- Consider **system-level** as well as entity-level classification

For Covered Entities

- **Self-assess** using the scoring methodology
- Identify applicable **obligations by tier**
- Plan for **phased compliance** based on tier assignment

For Technical Implementers

- Use obligation lists to **scope security programs**
- Design **shared services** (SOCs, audits) for Tier 2/3 entities
- Plan **incident reporting workflows** based on tier timelines

CII Case Studies: Digital Health Platforms

This chapter presents case studies for **digital health platforms** including national health information systems, personal health records, and hospital management information systems (HMIS).

Case Study 1: National Digital Health Platform - "SwasthyaSetu"

Entity Profile

Attribute	Details
Name	SwasthyaSetu (fictional national health ID platform)
Type	National digital health infrastructure
Operator	National Health Authority (government agency)
Coverage	800 million registered beneficiaries
Functions	Health ID issuance, consent management, health record linking, facility registry
Integrations	Connected to 50,000+ health facilities; insurance platforms; pharmacies
Employees	450 (central team)
Infrastructure	Multi-cloud; government data centers

CII Classification Assessment

Automatic Tier 1 Trigger Analysis

"Regardless of Size" Criterion	Applies?
Operates national-level health information system	☐
National health ID infrastructure	☐
Connected to national insurance platform	☐
Cross-sector dependencies (links to multiple sectors)	☐

Classification Result

Assessment	Result	Rationale
Automatic Tier 1	Yes	Meets multiple "regardless of size" triggers
Comparable to	National EHR/HIE systems globally	Similar to Singapore NEHR, UK NHS Spine

Applicable Obligations (Tier 1 - National System)

- **Governance**: Dedicated CISO + Security Operations Centre
- **Audit**: Continuous security monitoring; annual third-party audit; penetration testing
- **Incident reporting**: 12-hour early warning; 48-hour detailed notification
- **Business continuity**: Real-time disaster recovery; multi-region failover
- **Supply chain**: Rigorous vendor security assessment; cloud security requirements
- **Regulatory**: Direct reporting to national cyber authority
- **Exercises**: Mandatory participation in national/sectoral cyber drills

---

Case Study 2: Personal Health Record Platform - "My-HealthVault"

Entity Profile

Attribute	Details
Name	MyHealthVault
Type	Private consumer PHR/health data aggregation platform
Users	25 million registered users
Data aggregated	Lab reports, prescriptions, hospital records, wearable data
Integrations	Connected to 5,000+ labs, 2,000+ hospitals, 15 insurance companies
Employees	350
Revenue model	Freemium + B2B data analytics (anonymized)
Infrastructure	Multi-cloud (public cloud providers)
Special consideration	Aggregates data from multiple sources; consent-based sharing

CII Classification Assessment

Key Risk Factors

Factor	Assessment
Data volume	25M users $\times$ multiple records = billions of health data points
Data sensitivity	Complete longitudinal health records; genetic data for some users
Aggregation risk	Single breach exposes data from multiple source institutions
Third-party dependencies	Uses third-party APIs, cloud infrastructure, AI/ML partners

Factor	Assessment
Cross-border considerations	Some data processing in foreign jurisdictions

Scoring (Developing Country Framework)

Domain	Criterion	Points Scored
A. Scale	25M users (not case-based, but data scale)	25
B. Data Aggregation Risk	Centralized aggregation of distributed health data	20
C. Health System Integration	Connected to hospitals, labs, insurance	15
D. Consumer Dependency	Users rely on platform for health record access	10
TOTAL		**70**

Classification Result

Framework	Score	Tier	Rationale
Developing Country	70	**Tier 1 (Essential)**	Scale of data aggregation; integration with health ecosystem

> [!WARNING] PHR platforms present **unique aggregation risks** not captured by traditional facility-based metrics. A breach affects data originally held by thousands of source institutions. This case demonstrates why **data volume and aggregation** should be explicit scoring factors.

Applicable Obligations

- Dedicated CISO and DPO (Data Protection Officer)
- Annual third-party security audit + penetration testing
- 24-hour incident reporting for data breaches
- Consent management system audit
- Cloud vendor security assessment
- Cross-border data transfer compliance
- User notification protocols for breaches

Case Study 3: State HMIS Platform - "SwasthyaMitra"

Entity Profile

Attribute	Details
Name	SwasthyaMitra State HMIS Platform
Type	Hospital Management Information System serving state government hospitals
Operator	State Health Department (via NIC/state IT agency)
Coverage	500+ district hospitals, sub-district hospitals, and CHCs across the state
Users	45,000 healthcare workers; 800 facility administrators
Functions	Patient registration, OPD/IPD management, lab, pharmacy, billing, HMIS reporting
Data volume	15 million patient records; 50 million annual transactions
Infrastructure	State Data Center; hybrid cloud backup
Integrations	Connected to national ABDM, state insurance, disease surveillance, referral network
Special consideration	**Single platform for entire state public health system**

CII Classification Assessment

Key Risk Factors

Factor	Assessment
Scale	500+ facilities; single point of failure for state healthcare
Dependency	All state government hospitals depend on this platform
Data concentration	15M patient records in single system
Operational impact	Outage affects patient care statewide
Integration hub	Gateway to national systems (ABDM, insurance)

Scoring (Developing Country Framework)

Domain	Criterion	Points Scored
A. Scale	500+ facilities; 15M patient records	30
B. System Dependency	Single platform for all state public hospitals	25
C. Integration Role	Hub connecting facilities to national systems	15
D. User Base	45,000 healthcare workers depend on system	10

Domain	Criterion	Points Scored
TOTAL		**80**

Classification Result

Framework	Score	Tier	Rationale
Developing Country	80	**Tier 1 (Essential)**	State-wide system; single point of failure for 500+ facilities

[!IMPORTANT] Large-scale HMIS platforms serving hundreds of facilities are **system-level CII** regardless of whether individual facilities would independently qualify. The **concentration risk** of a shared platform elevates criticality significantly.

Applicable Obligations

- Dedicated security team (not just focal point)
- Continuous security monitoring (24/7 SOC)
- 12-24 hour incident reporting
- Disaster recovery with state-level failover
- Annual third-party penetration testing
- Change management security controls
- User access audit (45,000 users)
- API security for national integrations
- Backup and recovery testing (quarterly)
- Vendor security assessment (NIC/SI partners)

Case Study 4: Multi-Hospital HMIS - "CareSync Enterprise"

Entity Profile

Attribute	Details
Name	CareSync Enterprise HMIS
Type	Hospital Management Information System for private hospital group
Operator	CareSync Hospitals Private Limited
Coverage	5 large hospitals (average 400 beds each; 2,000 total beds)
Users	4,000 healthcare workers; 150 administrators
Functions	EMR, OPD/IPD, lab, radiology, pharmacy, billing, HR, analytics

Attribute	Details
Data volume	2 million patient records; 8 million annual transactions
Infrastructure	Private cloud; DR site
Integrations	Insurance TPA, ABDM, lab aggregators
Special consideration	**Centralized system for mid-size hospital chain**

CII Classification Assessment

Key Risk Factors

Factor	Assessment
Scale	5 hospitals; 2,000 beds total
Dependency	All 5 hospitals share single platform
Data concentration	2M patient records
Operational impact	Outage affects 5 facilities simultaneously
Market position	Regional player; not nationally critical

Scoring (Developing Country Framework)

Domain	Criterion	Points Scored
A. Scale	5 facilities; 2M patient records	20
B. System Dependency	Centralized platform for hospital chain	15
C. Geographic Criticality	Regional presence; alternative providers exist	5
D. National Integration	ABDM connected but not sole gateway	5
TOTAL		**45**

Classification Result

Framework	Score	Tier	Rationale
Developing Country	45	**Tier 2 (Important)**	Mid-scale platform; regional not national impact

[!NOTE] Smaller multi-hospital HMIS platforms like CareSync are **Tier 2** rather than Tier 1. The key differentiator from SwasthyaMitra is **scale and concentration**: 5 hospitals vs 500+, regional vs statewide impact, and presence of alternative providers.

Applicable Obligations

- Security focal point (may be shared CISO for group)
- Biennial third-party audit
- 72-96 hour incident reporting
- Business continuity plan with tested failover
- User access management
- Vendor security requirements
- ABDM integration security

Comparison: Large vs Small HMIS

Factor	SwasthyaMitra (Large)	CareSync (Small)
Facilities	500+	5
Patient records	15M	2M
Users	45,000	4,000
Geographic scope	State-wide	Regional
Alternative providers	No (sole state system)	Yes
Tier	**Tier 1**	**Tier 2**
Audit frequency	Annual	Biennial
Reporting timeline	12-24 hours	72-96 hours
SOC requirement	24/7 dedicated	Shared/outsourced

Summary: Digital Health Platform Classification

Case Study	Platform Type	Score	Tier
SwasthyaSetu	National digital health	Auto	**Tier 1** (auto)
MyHealthVault	PHR/health data aggregator	70	**Tier 1**
SwasthyaMitra	State HMIS (500+ hospitals)	80	**Tier 1**
CareSync Enterprise	Multi-hospital HMIS (5 hospitals)	45	**Tier 2**

Key Insights

1. **National platforms are automatic Tier 1**: Any national-level health information system triggers automatic classification
2. **Data aggregation creates concentrated risk**: PHR platforms aggregating from thousands of sources have unique criticality
3. **HMIS scale determines tier**: 500+ facilities is Tier 1; 5 facilities is Tier 2—a 100x difference justifies different classification
4. **System-level assessment matters**: A platform's criticality exceeds the sum of its connected facilities

CII Case Studies: Diagnostics, Pharma, and Biotech

This chapter presents case studies for **diagnostic services, pharmaceutical manufacturing, and biotechnology research** entities.

Case Study 1: Private Laboratory Chain - "DiagnoFirst"

Entity Profile

Attribute	Details
Name	DiagnoFirst Laboratory Network
Type	Private diagnostic laboratory chain
Coverage	500 collection centres; 25 processing labs
Tests performed	15 million per year
Employees	4,000
Key services	Pathology, radiology, molecular diagnostics
Digital systems	Centralized LIMS; patient portal; doctor portal
Integrations	Connected to 200+ hospitals; insurance platforms

CII Classification Assessment

Scoring (Developing Country Framework)

Domain	Criterion	Points Scored
A. Scale	15M tests/year (major national diagnostic player)	25
B. Capability	Reference laboratory for complex diagnostics	15
C. Geographic Criticality	Alternative labs available in most areas	5
D. National Program Integration	Disease surveillance contributor; insurance linked	15
TOTAL		**60**

Classification Result

Framework	Score	Tier	Rationale
Developing Country	60	**Tier 1 (Essential)**	Major diagnostic infrastructure; disease surveillance role

Applicable Obligations

- Group CISO for network
- Annual audit of centralized LIMS
- 24-48 hour incident reporting
- Supply chain security for IT vendors
- Data protection compliance (patient reports)

Case Study 2: Genomic Sequencing Laboratory - "GenomeIndia Labs"

Entity Profile

Attribute	Details
Name	GenomeIndia Labs
Type	Genomic sequencing and analysis laboratory
Operator	Public-private partnership (government + research institute)
Capacity	500,000 whole genome sequences/year
Data holdings	2 million genomic sequences (national population diversity project)
Services	Clinical genomics, research sequencing, population genomics
Key infrastructure	High-performance computing cluster; petabyte-scale storage
Integrations	Connected to national biobank, cancer registry, rare disease network
Special consideration	**National population genomic data asset**

CII Classification Assessment

Key Risk Factors

Factor	Assessment
Data uniqueness	Population-representative genomic data is irreplaceable national asset
Sensitivity	Genomic data is uniquely identifying and immutable
Research value	Supports drug development, disease research, personalized medicine
Sovereignty concern	Foreign access to population genomics is national security issue
Re-identification risk	Genomic data cannot be truly anonymized

Scoring (Developing Country Framework)

Domain	Criterion	Points Scored
A. Data Uniqueness	2M population genomic sequences (irreplaceable)	30
B. Data Sensitivity	Genomic data (highest sensitivity health data)	25
C. National Strategic Value	Population genomics as national asset	20
D. Research Infrastructure	Supports national health research ecosystem	10
TOTAL		**85**

Classification Result

Framework	Score	Tier	Rationale
Developing Country	85	**Tier 1 (Essential)**	National genomic data asset; highest sensitivity data type

[!CAUTION] Genomic data presents **unique risks** not fully captured by traditional health data frameworks. It is permanently identifying, affects biological relatives, and has sovereignty implications. Jurisdictions should consider **genomic-specific CII criteria**.

Applicable Obligations

- Dedicated CISO with research data security expertise
- Annual third-party audit including HPC infrastructure
- 24-hour incident reporting for any data exfiltration
- Access control: Tiered researcher access with approval workflow
- Data sovereignty: No unauthorized cross-border transfer
- Encryption: At-rest and in-transit for all genomic data
- Consent management audit
- International collaboration review (data sharing agreements)

Case Study 3: Vaccine Manufacturer - "BioShield Pharma"

Entity Profile

Attribute	Details
Name	BioShield Pharma Ltd.
Type	Vaccine and biologics manufacturer
Products	12 vaccines in portfolio (including childhood immunization, COVID-19)
Production capacity	500 million doses/year
Market share	35% of national vaccine supply; exports to 40 countries
Employees	8,000
Key systems	Manufacturing Execution System (MES), Quality Management System (QMS), Cold chain monitoring, Batch release systems
Regulatory status	WHO prequalified; national regulatory authority licensed
Special consideration	**Critical to national immunization program**

CII Classification Assessment

Automatic Tier 1 Trigger Analysis

"Regardless of Size" Criterion	Applies?
Critical to national immunization infrastructure	☐
Significant share (>20%) of essential medicine supply	☐
Export dependency by other countries	☐
Pandemic preparedness role	☐

Scoring (Using EU NIS2 Annex II-inspired criteria)

Domain	Criterion	Points Scored
A. Supply Criticality	35% of national vaccine supply	30
B. Manufacturing Scale	500M doses/year	25
C. Essential Medicine	Childhood immunization vaccines	20
D. Export/International	WHO prequalified; 40 countries depend	15
TOTAL		**90**

Classification Result

Framework	Score	Tier	Rationale
Developing Country	90	**Tier 1 (Essential)**	Critical national supply; automatic trigger for essential medicine manufacturing

[!NOTE] EU NIS2 Annex II explicitly includes **pharmaceutical manufacturers** and **medicinal products**. This case demonstrates applying supply-chain criticality metrics beyond traditional healthcare delivery.

Applicable Obligations

- Dedicated CISO with OT/ICS security expertise
- Annual audit of manufacturing systems (MES, QMS)
- 24-hour incident reporting for production disruptions
- Supply chain security for raw materials and packaging
- Business continuity: Redundant manufacturing capability
- Cold chain system monitoring and backup
- Coordination with national immunization program authority

Case Study 4: Biotech Research Company - "GeneSys BioTech"

Entity Profile

Attribute	Details
Name	GeneSys BioTech Private Limited
Type	Biotech research company developing biosimilars
Products in pipeline	8 biosimilars (oncology, autoimmune); 3 in Phase III trials
Key IP	Proprietary cell lines, manufacturing processes, clinical trial data
Employees	1,200
R&D investment	$150M cumulative in current pipeline
Key systems	Electronic Lab Notebook (ELN), Clinical Trial Management System (CTMS), IP database, Bioinformatics cluster
Partnerships	Licensing agreements with 3 multinational pharma companies

Attribute	Details
Special consideration	**High-value IP target; national biotech capability**

CII Classification Assessment

Key Risk Factors

Factor	Assessment
IP value	$150M+ R&D investment; biosimilar formulations are high-value targets
State-actor threat	Biosimilar development is target for economic espionage
National capability	One of few domestic companies with advanced biosimilar capability
Clinical data	Phase III trial data for thousands of patients
Supply chain	Potential future essential medicine supplier

Scoring (Developing Country Framework)

Domain	Criterion	Points Scored
A. IP/Data Sensitivity	Proprietary biosimilar formulations; cell lines	25
B. National Strategic Value	Domestic biotech capability; import substitution potential	20
C. Clinical Trial Data	Multi-thousand patient trial data	15
D. Future Supply Chain Role	Pipeline products for oncology/autoimmune	10
TOTAL		**70**

Classification Result

Framework	Score	Tier	Rationale
Developing Country	70	**Tier 1 (Essential)**	Strategic IP value; national biotech capability

[!IMPORTANT] This case illustrates **IP-based criticality** distinct from service delivery. Compromise of biosimilar development IP could set back national pharmaceutical capability by years and benefit foreign competitors. **Economic security** is a valid CII consideration.

Applicable Obligations

- Dedicated CISO with R&D security focus
- IP protection controls (access management, DLP, insider threat)
- Annual security audit including research systems
- 48-hour incident reporting (IP theft/exfiltration focus)
- Third-party research partner security assessment
- Bioinformatics infrastructure protection
- Secure collaboration protocols for international partners

Summary: Diagnostics, Pharma, and Biotech Classification

Case Study	Entity Type	Score	Tier
DiagnoFirst Labs	Private lab chain	60	**Tier 1**
GenomeIndia Labs	Genomic sequencing lab	85	**Tier 1**
BioShield Pharma	Vaccine manufacturer	90	**Tier 1** (auto)
GeneSys BioTech	Biotech (biosimilars IP)	70	**Tier 1**

Key Insights

1. **Major diagnostic chains are CII**: Laboratories with significant market share and disease surveillance roles qualify for Tier 1
2. **Genomic data has unique sovereignty implications**: Population genomics is a national asset requiring special protection
3. **Supply chain entities are CII**: Vaccine/pharma manufacturers with significant market share are Critical Infrastructure
4. **IP-based criticality is valid**: High-value biotech research IP warrants CII consideration for economic security

CII Case Studies: Public Health Programs and Surveillance

This chapter presents case studies for **national public health programs** including disease control programs, surveillance systems, and population health initiatives.

Case Study 1: Population-Based Surveillance System - "SurveilHealth"

Entity Profile

Attribute	Details
Name	SurveilHealth Integrated Disease Surveillance Platform
Type	National real-time disease surveillance and outbreak detection
Operator	National Centre for Disease Control (government)
Coverage	All 28 states; 750 districts; 150,000 reporting units
Functions	Real-time syndromic surveillance, outbreak detection, alert generation, response coordination
Data volume	50 million surveillance reports/year
Integrations	Laboratory network, hospital reporting, mortality surveillance, veterinary surveillance (One Health)
Response capability	Automated alert escalation; rapid response team coordination
Special consideration	**National epidemic response backbone**

CII Classification Assessment

Automatic Tier 1 Trigger Analysis

"Regardless of Size" Criterion	Applies?
National infectious disease surveillance	☑
Epidemic/pandemic response capability	☑
Public health emergency coordination	☑
One Health / cross-sector integration	☑

Scoring (Developing Country Framework)

Domain	Criterion	Points Scored
A. National Coverage	100% district coverage; 150,000 reporting points	30
B. Public Health Function	Epidemic detection and response	25
C. Real-time Criticality	Outbreak detection delays cost lives	20
D. Cross-sector Integration	One Health (human + animal surveillance)	10
TOTAL		**85**

Classification Result

Framework	Score	Tier	Rationale
Developing Country	85	**Tier 1 (Essential)**	National epidemic response backbone; automatic trigger

[!IMPORTANT] Population-based surveillance systems are **foundational pandemic preparedness infrastructure**. COVID-19 demonstrated that countries with robust surveillance detected outbreaks faster and responded more effectively. This is **non-negotiable Tier 1**.

Applicable Obligations

- Dedicated CISO + 24/7 Security Operations Centre
- Continuous security monitoring (real-time system criticality)
- 12-hour incident reporting (given outbreak detection dependency)
- Highly available infrastructure (multi-site redundancy)
- Data integrity controls (false data injection is attack vector)
- Integration security (APIs to laboratories, hospitals, veterinary)
- Annual penetration testing
- Participation in national cyber exercises

Case Study 2: National TB Elimination Program - "TB-Mukt Bharat"

Entity Profile

Attribute	Details
Name	TB-Mukt Bharat (National Tuberculosis Elimination Program)
Type	National disease control program
Operator	Central TB Division, Ministry of Health (government)
Coverage	All 28 states; 750 districts; 1.2 million+ DOTS providers
Annual notifications	2.5 million TB cases notified/year
Functions	Case notification, treatment tracking, drug resistance surveillance, contact tracing, preventive therapy
Key systems	Ni-kshay (national TB notification portal), drug logistics (DVS), lab network (RNTCP-NET)
Integrations	Linked to death registry, private sector portal, pharmacy dispensation, insurance
International obligations	WHO End TB Strategy reporting; Global Fund accountability
Special consideration	**India has highest TB burden globally; elimination target 2025**

CII Classification Assessment

Automatic Tier 1 Trigger Analysis

"Regardless of Size" Criterion	Applies?
National disease surveillance function	☐
Epidemic control program	☐
International reporting obligations	☐
Drug supply chain management	☐

Scoring (Developing Country Framework)

Domain	Criterion	Points Scored
A. National Coverage	100% district coverage; 2.5M cases/year	30
B. Public Health Function	TB elimination national priority	25
C. Drug Supply Chain	National TB drug procurement and distribution	15
D. International Accountability	WHO reporting; Global Fund grants	10
TOTAL		**80**

Classification Result

Framework	Score	Tier	Rationale
Developing Country	80	**Tier 1 (Essential)**	National TB elimination program; automatic trigger for disease surveillance

[!IMPORTANT] National disease control programs like TB-Mukt Bharat are **disease-specific critical infrastructure**. Disruption affects case detection, treatment continuity, drug supply, and international reporting. **Drug-resistant TB emergence** is a direct consequence of treatment disruption.

Applicable Obligations

- Dedicated program security officer
- Annual audit of Ni-kshay and connected systems
- 24-hour incident reporting (especially for supply chain disruption)
- Drug logistics system integrity monitoring
- Laboratory network data security
- Private sector portal integration security
- State-level IT node security coordination
- Data quality and integrity controls (false notifications are attack vector)

Case Study 3: National NCD Program - "Sankalp"

Entity Profile

Attribute	Details
Name	Sankalp (National Programme for Prevention and Control of NCDs)
Type	National non-communicable disease control program
Operator	NCD Division, Ministry of Health (government)
Coverage	700+ NCD clinics; 150,000+ HWCs for screening
Focus areas	Diabetes, hypertension, cancer, cardiovascular disease, stroke
Functions	Population screening, risk stratification, treatment protocols, follow-up tracking
Key systems	NCD App (screening/tracking), Cancer Registry integration, CPHC portal
Screenings	80 million population screened annually
Special consideration	**NCDs cause 62% of mortality in India**

CII Classification Assessment

Key Risk Factors

Factor	Assessment
Population coverage	80M annual screenings; lifetime chronic disease tracking
Continuity of care	Chronic disease management requires uninterrupted longitudinal tracking
Screening data	Early cancer/CVD detection depends on data integrity
Treatment continuity	Hypertension/diabetes patients require continuous medication access

Scoring (Developing Country Framework)

Domain	Criterion	Points Scored
A. Population Coverage	80M screenings/year across 700+ clinics	30
B. Public Health Function	NCDs are #1 mortality cause	20
C. Chronic Care Coordination	Longitudinal patient tracking essential	15
D. HWC Integration	150,000+ frontline facilities connected	10
TOTAL		**75**

Classification Result

Framework	Score	Tier	Rationale
Developing Country	75	**Tier 1 (Essential)**	Major national burden; population-scale screening and tracking

[!NOTE] NCD programs differ from acute disease programs in requiring **longitudinal data integrity over decades**. A patient's 10-year hypertension history affects current treatment decisions. Data corruption has delayed, but serious, consequences.

Applicable Obligations

- Program security focal point
- Annual audit of NCD App and connected systems
- 48-hour incident reporting
- Data integrity controls for longitudinal records
- HWC integration security (high-volume low-resource endpoints)
- Screening data backup and recovery
- Cancer registry linkage security

Case Study 4: National Blindness Control Program - "DrishtiRaksha"

Entity Profile

Attribute	Details
Name	DrishtiRaksha (National Programme for Control of Blindness & Visual Impairment)
Type	National eye care and blindness prevention program
Operator	Ophthalmology Division, Ministry of Health (government)
Coverage	District hospitals + 700 vision centres + school screening
Annual surgeries	7 million cataract surgeries/year (largest in world)
Functions	Cataract surgery tracking, school screening, IOL distribution, outcome monitoring
Key systems	NPCB-VI MIS, surgery outcome database, IOL inventory system
Integrations	District hospital systems, private eye hospital network
Special consideration	**World's largest cataract surgery program**

CII Classification Assessment

Key Risk Factors

Factor	Assessment
Surgery volume	7M surgeries/year; logistics coordination essential
Supply chain	IOL (intraocular lens) procurement and distribution
Outcome tracking	Post-surgical complication monitoring affects quality improvement
School screening	Detection of childhood visual impairment

Scoring (Developing Country Framework)

Domain	Criterion	Points Scored
A. Scale	7M surgeries/year; largest global program	25
B. Supply Chain	IOL procurement and distribution	15

Domain	Criterion	Points Scored
C. Outcome Monitoring	Quality assurance for surgical outcomes	10
D. School Health	Childhood screening program	10
TOTAL		**60**

Classification Result

Framework	Score	Tier	Rationale
Developing Country	60	**Tier 1 (Essential)**	Largest national surgical program; supply chain criticality

Applicable Obligations

- Program security focal point
- Annual audit of MIS and inventory systems
- 48-hour incident reporting
- IOL supply chain system monitoring
- Outcome database integrity controls
- School screening data protection
- Private hospital integration security

Case Study 5: National Nutrition Program - "Poshan Rakshak"

Entity Profile

Attribute	Details
Name	Poshan Rakshak (Integrated Child Development Services + POSHAN Abhiyaan)
Type	National nutrition supplementation and growth monitoring program
Operator	Ministry of Women and Child Development + Ministry of Health (joint)
Coverage	1.4 million Anganwadi centres; 14 crore children; 3.5 crore pregnant/lactating women

Attribute	Details
Functions	Growth monitoring, supplementary nutrition, immunization coordination, severe acute malnutrition (SAM) management
Key systems	ICDS-CAS (Common Application Software), Poshan Tracker, growth monitoring app, SAM referral system
Frontline workers	2.7 million Anganwadi workers with mobile devices
Integrations	Linked to immunization registry, MCTS (Mother and Child Tracking), hospital systems for SAM referrals
Special consideration	**Largest nutrition program globally; child survival dependency**

CII Classification Assessment

Automatic Tier 1 Trigger Analysis

"Regardless of Size" Criterion	Applies?
National child health program	☑
Life-critical for vulnerable populations (children, pregnant women)	☑
Supply chain for nutrition supplements	☑
Frontline health worker coordination	☑

Key Risk Factors

Factor	Assessment
Population	14 crore children + 3.5 crore PLW = 175M beneficiaries
Life-critical	SAM management prevents child deaths
Supply chain	Supplementary nutrition distribution
Data scale	2.7M frontline workers generating daily data
Integration complexity	Multi-ministry, multi-system integration

Scoring (Developing Country Framework)

Domain	Criterion	Points Scored
A. Beneficiary Scale	175M beneficiaries (children + PLW)	30
B. Life-Critical Function	SAM management; child survival	25
C. Supply Chain	Nutrition supplement distribution	15
D. Frontline Worker Coordination	2.7M Anganwadi workers	10
TOTAL		**80**

Classification Result

Framework	Score	Tier	Rationale
Developing Country	80	**Tier 1 (Essential)**	Largest nutrition program; child survival dependency; automatic trigger

[!CAUTION] Nutrition programs have **immediate life-safety implications for vulnerable populations**. Growth faltering detection delays directly increase child mortality. SAM referral system disruption is equivalent to emergency care disruption. This is **non-negotiable Tier 1**.

Applicable Obligations

- Dedicated program security officer
- Annual audit of Poshan Tracker and ICDS-CAS
- 24-hour incident reporting (given life-safety for children)
- SAM referral system high-availability requirements
- Supply chain system integrity monitoring
- Frontline worker device security (2.7M mobile endpoints)
- Multi-ministry coordination security protocols
- Growth data integrity controls (false data affects intervention targeting)
- Immunization linkage security

Summary: Public Health Program Classification

Case Study	Program Type	Score	Tier
SurveilHealth	Disease surveillance	85	**Tier 1** (auto)
TB-Mukt Bharat	TB elimination	80	**Tier 1** (auto)
Sankalp	NCD control	75	**Tier 1**
DrishtiRaksha	Blindness control	60	**Tier 1**
Poshan Rakshak	Nutrition/growth monitoring	80	**Tier 1** (auto)

Key Insights

1. **National surveillance is foundational CII**: Pandemic preparedness depends on surveillance system integrity
2. **Disease control programs have supply chain dependencies**: TB drugs, IOL distribution, nutrition supplements are attack vectors
3. **NCD programs need longitudinal integrity**: Chronic disease tracking requires decade-long data protection
4. **Child health programs are life-critical**: Nutrition monitoring and SAM referrals directly affect child mortality

5. **Frontline worker systems scale massively**: 2.7M devices create enormous endpoint security challenge

CII Case Studies: Registries, Biobanks, and Blood Services

This chapter presents case studies for **health data registries, biological sample repositories, and blood transfusion services**.

Case Study 1: National Cancer Registry - "OncoWatch"

Entity Profile

Attribute	Details
Name	OncoWatch National Cancer Registry
Type	National population-based cancer registry
Operator	National Institute of Cancer Research (government)
Coverage	95% population coverage across 28 states
Records	12 million cumulative cancer registrations since inception
Annual new cases	1.4 million new registrations/year
Data elements	Demographics, diagnosis, staging, treatment, outcomes, mortality
Integrations	Linked to death registry, hospital cancer departments, pathology labs
Uses	National cancer control planning; research; epidemiology

CII Classification Assessment

Automatic Tier 1 Trigger Analysis

"Regardless of Size" Criterion	Applies?
National-level health information system	☐
Disease surveillance function	☐
Public health planning dependency	☐
Research infrastructure	☐

Scoring (Developing Country Framework)

Domain	Criterion	Points Scored
A. Population Coverage	95% national coverage	30

Domain	Criterion	Points Scored
B. Data Sensitivity	12M cancer patient records with outcomes	25
C. Public Health Function	National cancer control planning	20
D. Research Infrastructure	Supports national/international cancer research	10
TOTAL		**85**

Classification Result

Framework	Score	Tier	Rationale
Developing Country	85	**Tier 1 (Essential)**	National disease registry; public health planning dependency

Applicable Obligations

- Dedicated security officer
- Annual audit with focus on data integrity (registry accuracy is critical)
- 24-hour incident reporting
- Access control audit (researcher access management)
- Backup and recovery testing (longitudinal data irreplaceable)
- Data sharing agreement security review
- International collaboration security protocols

Case Study 2: National Biobank - "JeevanKosh"

Entity Profile

Attribute	Details
Name	JeevanKosh National Biobank
Type	National biological sample and data repository
Operator	National Institute of Biomedical Research (government)
Sample holdings	5 million biological samples (blood, tissue, DNA)
Linked data	Clinical phenotypes, genomic data, longitudinal health outcomes

Attribute	Details
Sources	Population cohorts, disease-specific studies, hospital contributions
Access	Enables national and international research collaborations
Infrastructure	Automated sample storage (-80°C, liquid nitrogen); LIMS; linked databases
Special consideration	**Irreplaceable national research resource**

CII Classification Assessment

Key Risk Factors

Factor	Assessment
Sample irreplaceability	Samples from deceased donors or rare disease patients cannot be recreated
Linked data sensitivity	Samples linked to genomic, clinical, and outcome data
Physical + cyber risks	Both physical sample security and data security required
Research dependency	National health research ecosystem depends on biobank access
Consent complexity	Samples collected under specific consent; breach affects consent validity

Scoring (Developing Country Framework)

Domain	Criterion	Points Scored
A. Sample Volume	5M biological samples	25
B. Data Sensitivity	Linked genomic + clinical data	25
C. Irreplaceability	Samples from discontinued cohorts, deceased donors	20
D. Research Infrastructure	National research ecosystem dependency	15
TOTAL		**85**

Classification Result

Framework	Score	Tier	Rationale
Developing Country	85	**Tier 1 (Essential)**	Irreplaceable national research resource; linked sensitive data

> [!NOTE] Biobanks present **hybrid physical-cyber security requirements**. Loss of sample integrity (physical) or linked data (cyber) both constitute major incidents. CII frameworks should explicitly address **biobank-specific criteria**.

Applicable Obligations

- Dedicated security officer (physical + cyber)
- Annual audit covering both physical and IT security
- 24-hour incident reporting (including physical security events)
- Sample tracking integrity controls
- Access management for researchers (physical + data)
- Backup and disaster recovery for LIMS
- Consent management system security
- Third-party researcher security assessment
- International collaboration data transfer controls

Case Study 3: State Blood Transfusion Council - "Jeevan Raksha"

Entity Profile

Attribute	Details
Name	Jeevan Raksha State Blood Transfusion Council
Type	State-level blood transfusion coordination agency
Coverage	28 districts; coordinates 45 blood banks
Functions	Blood inventory management, donor registry, cross-matching coordination
Population served	50 million
Employees	85
Digital systems	State blood bank management system; real-time inventory
Connectivity	Connected to all district blood banks

CII Classification Assessment

Automatic Tier 1 Trigger Analysis

"Regardless of Size" Criterion	Applies?
Operates blood allocation services at regional level	☐
Single point of coordination for state blood supply	☐
Life-critical dependency (emergency transfusions)	☐

142

Scoring (Developing Country Framework)

Domain	Criterion	Points Scored
A. Scale	Not applicable (coordination agency)	0
B. Public System Role	State-level life-critical service	25
C. Geographic Criticality	Single coordination point for state	20
D. Functions	Blood bank coordination (life-critical)	25
TOTAL		**70**

Classification Result

Assessment	Result	Rationale
Score-based	70 → Tier 1	High score on function and uniqueness
Automatic Tier 1	Yes	Blood supply coordination is automatic trigger

Applicable Obligations

- Dedicated security officer
- Real-time monitoring of blood inventory system
- 24-hour incident reporting (supply chain disruption)
- Business continuity: Manual fallback for blood matching/allocation
- Annual audit with focus on data integrity

Summary: Registries, Biobanks, and Blood Services Classification

Case Study	Entity Type	Score	Tier
OncoWatch	National cancer registry	85	**Tier 1** (auto)
JeevanKosh	National biobank	85	**Tier 1**
Jeevan Raksha	State blood coordination	70	**Tier 1** (auto)

Key Insights

1. **Disease registries support public health planning**: National registry data is irreplaceable and supports policy decisions

2. **Biobanks need hybrid security**: Physical sample integrity + cyber data protection are equally critical
3. **Blood services are life-critical**: Real-time coordination for emergency transfusions has immediate mortality implications
4. **Longitudinal data is irreplaceable**: Decades of registry/biobank data cannot be reconstructed after loss