Comprehensive Guide to Incident Response

A step-by-step playbook for detecting, containing, and recovering from cyberattacks

Contents

[Abbreviations ii](#_Toc210217929)

[Key definitions III](#_Toc210217930)

[Introduction 2](#_Toc210217931)

[Purpose 2](#_Toc210217932)

[Objectives of this guide 3](#_Toc210217933)

[Target audience 3](#_Toc210217934)

[Understanding cybersecurity incidents 3](#_Toc210217935)

[Incident response planning: Why it is essential 7](#_Toc210217936)

[Communication, documentation, tools, and considerations 10](#_Toc210217937)

[Appendix A: Sample incident response checklist 13](#_Toc210217938)

[Appendix B: Real-world examples of cybersecurity incidents 14](#_Toc210217939)

# Abbreviations

APT Advanced Persistent Threat

DDoS Distributed Denial-of-Service

DoS Denial-of-Service

EMR electronic medical record

GDPR General Data Protection Regulation

HIPAA Health Insurance Portability and Accountability Act

IDS intrusion detection system

IPS intrusion prevention system

IR incident response

IRP incident response plan

IT information technology

LMIC low- and middle-income countries

MOH ministry of health

NDR National Data Repository

NHLS National Health Laboratory Service

NIST National Institute of Standards and Technology

NIS2 Network and Information Systems Directive 2

TAP Technical Assistance Platform

# Key definitions

* **Breach**: An incident that results in confirmed disclosure of data to an unauthorized party.
* **Cyberattack**: A deliberate attempt to damage, disrupt, or gain unauthorized access to computer systems, networks, or data.
* **Cybersecurity**: The practice of protecting systems, networks, and programs from digital attacks aimed at accessing, changing, or destroying sensitive information.
* **Event**: Any observable occurrence in a system or network.
* **Incident**: An attempted or actual unauthorized access, use, disclosure, modification, or destruction of information.
* **Malware**: Software designed to disrupt, damage, or gain unauthorized access to a computer system.
* **Phishing**: A fraudulent attempt to obtain sensitive information by disguising as a trustworthy entity in electronic communication, typically via email.
* **Ransomware**: A type of malware that encrypts files on a victim's system and demands payment (usually in cryptocurrency) for the decryption key.
* **Advanced Persistent Threat (APT)**: A prolonged and targeted cyberattack in which an intruder gains access to a network and remains undetected for an extended period.
* **Denial-of-Service (DoS)**: An attack that aims to shut down a machine or network, making it inaccessible to its intended users.
* **Distributed Denial-of-Service (DDoS)**: A DoS attack that uses multiple compromised systems to flood the target with traffic.
* **Insider threat**: A security risk that originates from within the organization, such as from employees, contractors, or partners.
* **Social engineering**: The psychological manipulation of people into performing actions or divulging confidential information.

Introduction

Ministries of health (MOHs) and implementing partners increasingly rely on digital health systems to store and process sensitive health data. Cybersecurity incidents—such as ransomware, unauthorized access, or data breaches—can disrupt services, compromise patient safety, and cause significant legal and reputational harm. This playbook provides a step-by-step guide for incident response, aimed at enhancing cybersecurity readiness, facilitating ownership and sustainability, protecting health data and services, standardizing incident response, and promoting long-term resilience.

In today’s digital health landscape, global health programs are more reliant than ever on electronic systems to deliver care, manage data, and coordinate across borders. This interconnectedness, while essential, also exposes these programs to rising cybersecurity threats, which can jeopardize patient safety, disrupt services, and erode public trust.

For example, under the US Centers for Disease Control and Prevention-funded Technical Assistance Platform (TAP) project, collaborations with MOHs and other stakeholders have led to the development and deployment of critical systems such as electronic medical records (EMRs), National Data Repositories (NDRs), and Patient Identity Management Systems. While these systems strengthen data-driven decision-making and continuity of care, they also significantly expand the digital attack surface.

A robust risk management strategy is no longer optional—it is foundational. It helps programs anticipate vulnerabilities, prioritize protection of sensitive health information, and ensure continuity in emergencies. Central to this strategy is an Incident Response (IR) guide, which equips teams with a clear, step-by-step playbook for detecting, containing, and recovering from cyberattacks. In a high-stakes environment where resources are often limited, a well-prepared IR guide turns chaos into coordination, enabling faster recovery and minimizing harm.

Purpose

Incident response in cybersecurity extends far beyond basic damage control; it is foundational to the resilience of health systems. Especially within global health, the purpose of incident response is to detect, contain, mitigate, recover from, and learn from cybersecurity incidents. This proactive approach protects the confidentiality, integrity, and availability of sensitive health information. By aiming to minimize operational impact and financial loss, maintain compliance with data protection laws such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA), and ensure the continuity of essential health services, incident response helps organizations swiftly detect root causes, restore systems, and safeguard their reputation. Ultimately, effective incident response is essential to sustaining the trust and reliability that are central to digital health initiatives.

Objectives of this guide

* **Enhance cybersecurity readiness**: Provide a structured, cost-effective framework tailored to African health settings to help health teams detect, contain, and recover from cyber threats using local tools and skills.
* **Facilitate ownership and sustainability**: Empower MOHs and local stakeholders with the resources to manage and safeguard TAP-developed systems (EMRs, NDRs, Patient Identity Management Systems) as they transition to full ownership.
* **Protect health data and services**: Implement practical, context-specific measures to minimize service disruptions and ensure the confidentiality, integrity, and availability of sensitive health information, including scenario-based planning for contextual infrastructure limitations.
* **Standardize and localize incident response**: Establish a consistent, adaptable approach to managing cyber incidents aligned with global best practices and local realities.
* **Promote long-term resilience**: Foster a security-first culture that strengthens institutional capacity and ensures the sustainability of national digital health assets through community-driven security awareness programs.

Target audience

This guide is intended for ministries of health and implementing partners investing in digital health platforms in low- and middle-income countries (LMICs). It is particularly aimed at health information technology (IT) professionals and security teams, public health administrators, and hospital and laboratory network managers, including those operating national or regional eHealth systems.

Understanding cybersecurity incidents

What is Incident Response?

Incident Response (IR) is a structured, systematic approach to managing and mitigating the aftermath of a cybersecurity incident or breach. The goal is to handle the situation in a way that limits damage, reduces recovery time and costs, and prevents future incidents.

What are cybersecurity incidents?

A cybersecurity incident is any event that threatens the confidentiality, integrity, or availability of an organization’s systems, data, or networks. For example, on June 22, 2024, the BlackSuit ransomware gang targeted South Africa’s National Health Laboratory Service (NHLS)—a network of 256 laboratories—encrypting systems and shutting down critical infrastructure. Operations like email, website access, and electronic lab result retrieval were taken offline. This attack rendered the public health sector’s test orders, results, and historical data inaccessible, compromising over 1.2 terabytes of data, including patient information. Apart from highlighting the vulnerability of public health data systems, this attack (and many others like it) underscores the need for appropriate cybersecurity measures and incident response plans in the healthcare sector.

Types of cybersecurity incidents

To effectively respond to incidents, you need to understand the types of threats you might encounter.

### **Malware attacks:** Malware, or malicious software, is designed to infiltrate and damage systems and disrupt business operations. Some of the most dangerous types include:

* Viruses: Infect and spread by attaching to legitimate programs.
* Worms: Self-replicating programs that spread across networks without user action.
* Ransomware: A type of malware that encrypts your data and demands a ransom for its release.

### **Phishing and social engineering:** Cybercriminals use deception to manipulate individuals into providing sensitive information or granting unauthorized access. Common tactics include:

* Phishing emails: Fraudulent emails pretending to be from legitimate sources.
* Spear phishing: Targeted attacks on specific individuals (e.g., executives).
* Business email compromise: Attackers impersonate company executives to trick employees into transferring funds.[[1]](#footnote-2)

1. **Data breaches:** A data breach occurs when unauthorized individuals gain access to sensitive information, such as patient data, financial records, or trade secrets.
2. **Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks:** Attacks that overwhelm your systems with traffic, causing them to crash. For instance, hackers flood a website or network with excessive traffic, which causes slowdowns or complete outages.

* DoS attacks: Single-source attack that overwhelms a system.
* DDoS attacks: Large-scale attacks using multiple compromised devices (botnets).

1. **Insider threats:** Not all threats come from outside—insider threats involve employees, contractors, or partners. These can be:

* Malicious insiders: Employees who intentionally steal data or sabotage systems.
* Negligent insiders: Employees who accidentally expose sensitive data through weak security practices.

Other incident types include supply chain attacks, cloud security incidents, and advanced persistent threats (APTs). Each incident type may require a slightly different containment and eradication strategy. Appendix B contains real-world cybersecurity incident examples.

How to identify security incidents

To identify security incidents in digital health systems, organizations must implement a combination of automated monitoring tools, user behavior analytics, and staff awareness. This includes using intrusion detection systems (IDS), antivirus logs, access control audits, and real-time alerts to flag anomalies such as unauthorized logins, unusual data transfers, system slowdowns, or sudden configuration changes. Human observation also plays a key role—frontline users reporting strange pop-ups, locked files, or suspicious emails can provide early warning of threats like ransomware or phishing. Importantly, security incidents must be clearly defined in policy, and all staff should know how and when to report them to ensure rapid response and minimize impact. Figure 1 (below) illustrates frequent signs of cybersecurity compromise.

Figure 1. Incident indicators in cybersecurity.

A diagram of information on a computer

AI-generated content may be incorrect.

Common indicators of incidents:

* Unusual network traffic patterns, like unexpected spikes in traffic or unauthorized access attempts.
* Suspicious login attempts or account activity: possible brute-force attack or compromised credentials.
* Unexpected system performance degradation.
* Unauthorized changes to files or system configurations: unknown software installations or configuration changes.
* Unusual security alerts or error messages.
* Suspicious emails or links: potential phishing or malware distribution.

Understanding false positives vs. true incidents:

* Distinguishing between legitimate alerts and actual security breaches is critical.
* Requires careful analysis of logs, patterns, and contextual information.

Why is incident response necessary?

Cyber incidents in digital health systems have far-reaching and often life-threatening impacts, affecting not just data and IT infrastructure but also patient safety, health service delivery, and continuity of care, public trust, and global health security.

Cyberattacks impact many areas in health. Table 1 (below) highlights the impact areas with accompanying consequences (Also refer to *Appendix B: Real-world examples of cybersecurity incidents*).

Table 1. Consequences of Cyber Attacks on Digital Health.

|  |  |
| --- | --- |
| Impact area | Consequences |
| Patient safety & care | Delays in treatment, misdiagnosis, disrupted care continuity, and potential fatalities. |
| Service delivery disruption | Outages in EMR, lab systems, supply chain, and telehealth services. |
| Data breach & privacy loss | Exposure of sensitive health data leading to stigmatization, discrimination, and loss of legal compliance. |
| Financial & resource drain | Ransom payments, recovery costs, funding loss, and diversion of critical funds from health services.[[2]](#footnote-3) |
| Legal, regulatory, and donor fallout | Contract violations, failed audits, loss of donor confidence. Example: Violations of the European GDPR, HIPAA, or, in Africa, local Data Protection Acts such as the Democratic Republic of the Congo’s Code de Numerique (2023). A concrete example is that of the French data protection authority (CNIL) which issued a fine of €400,000 to AP-HP (Assistance Publique–Hôpitaux de Paris) in 2021 after a data breach exposed health data of 1.4 million COVID-19 test subjects.[[3]](#footnote-4) |
| Erosion of public trust | Reduced use of digital health tools, vaccine hesitancy, loss of patient trust, and business credibility. Example: Singapore’s largest health care group, SingHealth, suffered a massive cyberattack where personal data of 1.5 million patients—including the Prime Minister—was stolen.[[4]](#footnote-5) |
| Setback to health outcomes | Slowed progress toward health goals and equity |
| Staff burnout & psychological strain | Stress and fatigue during prolonged recovery efforts |
| Increased targeting of LMICs | Higher vulnerability to sophisticated, resource-intensive cyberattacks |

Incident response planning: Why it is essential

An incident response plan (IRP) is a structured document that outlines how an organization detects, responds to, and recovers from security incidents (See Figure 2). Without a plan, teams scramble to react, increasing damage, downtime, and financial loss.

Figure 2. Advantages of Incident Response Planning.

Diagram of an umbrella

AI-generated content may be incorrect.

Creating an effective incident response plan

The IR Manager (See IR Team, below) leads the development of the incident response plan. A solid IRP includes detailed response steps, communication protocols, and team responsibilities. It should be tailored to an organization’s size, industry, and risk profile.

Define the scope of the plan

* Identify critical assets, systems, and data that require protection.
* Determine which types of incidents the IRP will cover (e.g., malware, insider threats).
* Define incident response steps: Align with the Incident Response Lifecycle (Preparation → Identification → Containment, etc.).
* Establish escalation procedures: Determine when and how to involve leadership, legal teams, and external experts.
* Test and update regularly: Run tabletop exercises and penetration tests to validate effectiveness.

Incident Response team

Central to IR is designating a Security Operations Center or establishing an IR team. This cross-functional team will implement IR measures to detect, contain, and recover from cyberattacks. This team is led by the IR manager. Table 2 (below) shows various roles and responsibilities of IR team.

Table 2. Responsibilities of an IR team.

|  |  |
| --- | --- |
| Role | Responsibilities |
| IR manager | Leads the response: oversees the entire IR process, coordinates resources, and ensures communication flow. |
| Forensics analyst | Investigates threats, analyzes logs, and identifies attack vectors. |
| IT/Network engineer | Executes containment and recovery. |
| Security analysts | Detects, analyzes, and responds to incidents using technical tools and threat intelligence. |
| System administrators | Assists in containment, eradication, and recovery tasks. |
| Legal/compliance team | Ensures regulatory requirements and ensure legal obligations are met. |
| Communication officer | Manages internal and external communications, including public relations if necessary. |
| Executive sponsor | Makes high-level business decisions regarding impact and resource allocation. |

The 6-Phase Incident Response lifecycle

The IR lifecycle is often modeled after the National Institute of Standards and Technology (NIST) 800-61 framework and consists of six critical phases: Preparation → Identification → Containment → Eradication → Recovery → Lessons Learned/Post-incident.

A structured IR lifecycle ensures that organizations can efficiently detect, contain, and recover from cyber threats (See Figure 3). Following a well-defined six-phase approach minimizes damage, reduces downtime, and strengthens future defenses.

Figure 3. Incident Response Lifecycle.

A diagram of a fire response lifecycle

AI-generated content may be incorrect.

Phase 1: Preparation

**Objective:** Build organizational readiness to manage incidents. Develop an IRP, define roles and responsibilities, assemble an IR Team, and establish communication protocols. Regular training and monitoring setups are vital. Activities during this phase include:

* Develop an IRP.
* Define roles and responsibilities.
* Assemble an IR team.
* Establish communication protocols.
* Deploy security tools: intrusion detection systems (IDS) and intrusion prevention systems (IPS), security information and event management, and endpoint detection.
* Conduct regular training and desktop exercises.
* Create an asset inventory and risk assessment baseline.
* Establish secure logging, monitoring, and data retention strategies.
* Develop an incident classification and prioritization matrix.

Phase 2: Identification

**Objective:** Identify and confirm potential security incidents through logs, threat intelligence, and forensic validation.

* Monitor systems for anomalies, alerts, and threat intelligence.
* Use log analysis, network forensics, and automated tools.
* Validate suspected incidents using a combination of:
  + Signature-based detection.
  + Anomaly-based detection.
  + Behavior-based analytics.
* Document the following:
  + Who identified the incident.
  + Date and time of detection.
  + Systems involved.
  + Initial impact assessment.
  + Attack vectors.

Phase 3: Containment

**Objective:** Limit the spread and impact of the incident. Short-term isolation and long-term hardening are critical.

Short-term containment requires:

* Isolation of the affected systems.
* Disablement of compromised accounts.
* Application of temporary firewall rules or segmentation.

Long-term containment involves:

* Patching vulnerable systems and changing credentials.
* Hardening configurations
* Monitoring for lateral movement.

Best practices include avoiding tipping off attackers, preserving evidence for legal and forensic review, and documenting all actions taken. Where applicable (i.e., specified in accordance with in-country personal health data protection legislation), notify the Office of the Data Protection Authority or equivalent of the incident within the timeframe specified, considering any relevant steps to inform data subjects in line with data subject rights.

Phase 4: Eradication

**Objective:** Remove root causes and artifacts. Patching, forensic review, and validation of integrity follow.

* Identify and remove malware, backdoors, and unauthorized accounts.
* Apply security patches and updates.
* Verify the integrity of affected systems.
* Conduct root cause analysis to ensure complete eradication.
* Engage digital forensics if necessary.

Phase 5: Recovery

**Objective:** Restore systems to normal operation, monitor for weaknesses, and ensure proper functionality before resuming normal operations.

* Restore systems from clean backups.
* Rebuild compromised systems if necessary.
* Validate system functionality.
* Monitor systems for signs of recurring attacks.
* Remove temporary containment measures.
* Conduct post-restoration testing.

Phase 6: Lessons learned/post-incident

**Objective:** Strengthen defenses based on retrospective analysis. Document timelines, findings, and recommendations.

* Conduct a post-incident review within 1–2 weeks.
* Identify:
* What went wrong and right?
* Any potential improvements.
* Update IR policies, security controls, and training.
* Share de-identified findings with relevant stakeholders.
* Document timelines, technical details, and financial impacts.

Communication, documentation, tools, and considerations

Communication, documentation, tools and technologies, regulatory and legal considerations, as well as ensuring continuous improvement, are some essential activities for a successful IR.

Communication plan

A communications plan is a crucial component of an effective cybersecurity IR, ensuring the timely, accurate, and transparent sharing of information during a crisis. It serves as a roadmap for coordinating internal and external communications, minimizing confusion, and maintaining stakeholder trust. By outlining clear protocols for who communicates what, when, and to whom, the plan helps organizations manage the narrative, comply with regulatory requirements, and mitigate reputational damage.

* Internal communication: Secure channels like encrypted emails, Signal, or Slack with multi-factor authentication.
* External communication: Pre-approved templates for media, partners, and regulators.
* Reporting: Define what to report, when, and to whom (e.g., legal counsel, authorities, customers).

Documentation and evidence handling

Comprehensive documentation provides a detailed record of the incident timeline, actions taken, and systems affected, supporting accurate analysis and informed decision-making. Proper evidence handling ensures the integrity and admissibility of digital artifacts, such as logs, network traffic, or compromised files, which are critical for identifying attack vectors, attributing responsibility, and meeting legal or regulatory requirements.

* Use standardized incident report templates.
* Maintain an incident log including incident timeline, decisions made, and actions taken.
* Preserve digital evidence in accordance with chain-of-custody principles.[[5]](#footnote-6)
* Use write-blockers and forensic imaging for disk captures.

Tools and technologies

Advanced solutions, such as intrusion detection systems, endpoint protection platforms, and forensic analysis tools, enable rapid identification of malicious activities and provide critical insights into the scope and nature of an attack. These technologies facilitate automated responses, real-time monitoring, and secure evidence collection, significantly reducing response times and minimizing damage. By leveraging cutting-edge tools, organizations can enhance their ability to contain incidents, recover systems efficiently, and build robust defenses against evolving cyber threats. Some tools and technologies to consider:

* Security information and event management platforms.
* Endpoint detection and response / Extended detection and response.
* Network Forensics: Tools like Wireshark and Zeek.
* Threat intelligence platforms.
* Automation: Security orchestration, automation, and response.

Regulatory and legal considerations

Adhering to regulations governs how sensitive data breaches are reported, investigated, and mitigated, helping avoid penalties and legal liabilities. A clear understanding of these obligations guides timely notifications to authorities and affected parties, maintains transparency, and upholds stakeholder trust.

* Understand and comply with GDPR, HIPAA, Network and Information Systems Directive 2 (NIS2), and relevant local cybercrime legislation.
* Maintain breach notification templates.
* Work with legal counsel to assess liability and reporting obligations.

Continuous improvement

By regularly reviewing and refining response processes, analyzing past incidents, and incorporating lessons learned, teams can identify gaps, streamline procedures, and improve reaction times. This iterative approach fosters resilience, strengthens coordination, and ensures that strategies remain effective against emerging attack vectors. It is advisable to:

* Conduct regular IR drills.
* Review and update the Incident Response Plan biannually.
* Analyze security trends and threat intelligence.
* Foster a security-aware culture within the organization.

Indicators for measuring success

Success in IR can be measured through key performance indicators such as:

* Mean time to detect: Average time from incident occurrence to detection; aim for under 24 hours.
* Mean time to respond: Average time to contain and eradicate; target less than 48 hours.
* Incident resolution rate: Percentage of incidents fully resolved without recurrence within 30 days.
* Downtime reduction: Decrease in service disruptions compared to previous incidents.
* Compliance adherence: Number of incidents where regulatory notifications were met on time.
* Training effectiveness: Post-drill surveys showing improved team readiness scores.
* Cost savings: Reduction in financial impact per incident through faster recovery.

These indicators should be tracked quarterly and used to refine the IRP.

Conclusion

IR is not a reactive task; it is an ongoing commitment. A mature and well-tested IR program not only mitigates damage, but builds resilience and trust across your organization and stakeholder network.

Appendix A: Sample incident response checklist

This page serves as a rapid reference for immediate incident response actions. It should be printed and made available to all key team members.

**🔔 IMMEDIATE ACTIONS CHECKLIST**

|  |  |  |
| --- | --- | --- |
| **Task** | **Responsible** | **Status** |
| 1. Identify and classify the incident | Security analyst | ☐ |
| 2. Notify IR manager | First responder | ☐ |
| 3. Inform executive sponsor and legal team | IR manager | ☐ |
| 4. Isolate affected systems/accounts | IT admin | ☐ |
| 5. Activate containment protocols | IR team | ☐ |
| 6. Collect & preserve digital evidence (screenshots, logs) | Forensics analyst | ☐ |
| 7. Initiate communication plan (internal/external) | Communications officer | ☐ |
| 8. Eradicate root cause | Forensics analyst | ☐ |
| 9. Recover systems and validate | IT admin | ☐ |
| 10. Conduct lessons learned review | IR manager | ☐ |
| * 1. Update policies and training | IR manager | ☐ |

**📞 EMERGENCY CONTACTS**

* IR manager: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* Legal/compliance contact: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* Communications lead: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**📂 KEY DOCUMENTS & LOCATIONS**

* Incident response policy: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* Backup directory: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* Contact directory: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* Evidence log template: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Appendix B: Real-world examples of cybersecurity incidents

|  |  |  |  |
| --- | --- | --- | --- |
| Incident type | Location | Description | Impact |
| Malware /  Ransomware | NHLS Ransomware Attack  (South Africa, 2024) | BlackSuit ransomware encrypted systems in 256 laboratories, shutting down email, websites, and lab results access. Over 1.2 TB of patient data compromised.  Targeting digital health systems (e.g., NHLS in South Africa) [^1] | Disrupted public health testing, inaccessible historical data, potential patient privacy violations. |
| Ransomware | WannaCry Ransomware  (Global, 2017) | Affected the UK's National Health Service (NHS), encrypting data on thousands of computers. | Canceled surgeries and appointments, estimated at £92 million in costs, highlighted vulnerabilities in outdated systems. |
| Ransomware | Change Healthcare Breach  (USA, 2024) | Ransomware attack on a major U.S. health payment processor, exposing sensitive data of millions. | Disrupted billing and claims processing, financial strain on providers, potential identity theft for patients. |
| Phishing | Bangladesh Bank  (Heist, 2016) | APT involving phishing and SWIFT network compromise, stealing $81 million. | Financial loss, erosion of trust in banking systems used for health funding. |
| Supply chain attack |  | Software vendors serving multiple LMICs may be targeted. |  |
| Insider threats |  | Local clinic staff accidentally exposing data via USB devices [^6] |  |
| Denial of Services  (DoS/DDoS) |  | My Health Record platform in Australia disrupted by floods of access requests [^4] |  |
| Phishing |  | WHO staff targeted during COVID-19 via fake update emails [^2] |  |
| Data breach |  | WHO staff targeted during COVID-19 via fake update emails [^2] |  |

1. Vuk’uzenzele (2016). High scam alert to suppliers and service providers of the Department of Health. https://www.vukuzenzele.gov.za/high-scam-alert-suppliers-and-service-providers-dept-health [↑](#footnote-ref-2)
2. UK National Audit Office (2018). *Investigation: WannaCry cyber attack and the NHS*. NAO report [↑](#footnote-ref-3)
3. CNIL. (2022). Sanction décision against AP-HP. Sanction décision against AP-HP [↑](#footnote-ref-4)
4. Cyber Security Agency of Singapore. (2019). Public Inquiry Report on SingHealth Cyber Attack [↑](#footnote-ref-5)
5. A detailed, chronological record that tracks evidence from its collection through its handling, storage, and final disposition. Its purpose is to ensure the evidence's legal integrity and authenticity by documenting every person who handled it, when, and where, which prevents contamination, tampering, misplacement, or alteration. [↑](#footnote-ref-6)