Indian Health Service

Protecting Patient Health Information

REESE WEBER, MBA, CISSP

2026 BEST PRACTICES VIRTUAL SERIES

Agenda

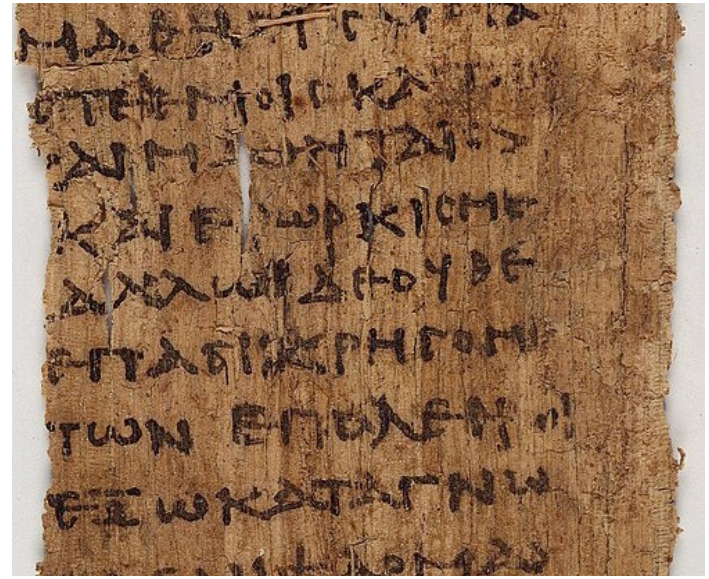
- Introduction
- HIPAA Overview
- Cybersecurity Risks
- Access Controls
- Clinical Workflow Integration
- Compliance
- Case Study
- Discussion/Questions

An Ancient Greek Approach to Medical Data Privacy

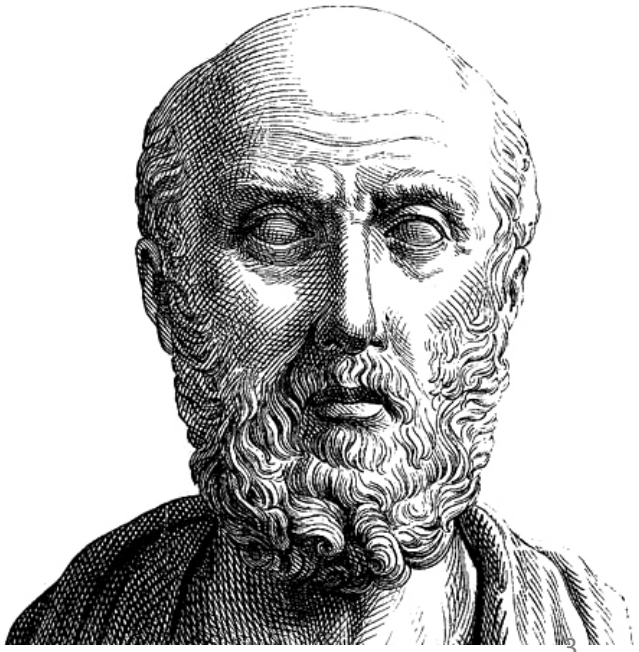
The Hippocratic Oath

The **Hippocratic Oath** is a traditional ethical pledge historically taken by physicians. Originating in ancient Greece and (probably inaccurately) attributed to Hippocrates, it emphasizes a healthcare provider's duty to practice medicine ethically, protect patient confidentiality, avoid causing harm, and prioritize patient well-being. Modern versions of the oath continue to guide medical professionalism, compassion, integrity, and responsibility in patient care.

"Whatever, in connection with my professional practice or not, in connection with it, I see or hear, in the life of men, which ought not to be spoken of abroad, I will not divulge, as reckoning that all such should be kept secret."



A fragment of the oath on the 3rd-century Papyrus Oxyrhynchus 2547



The Greek physician Hippocrates

Why Patient Data Protection Matters

Patient trust and confidentiality

Legal and financial implications

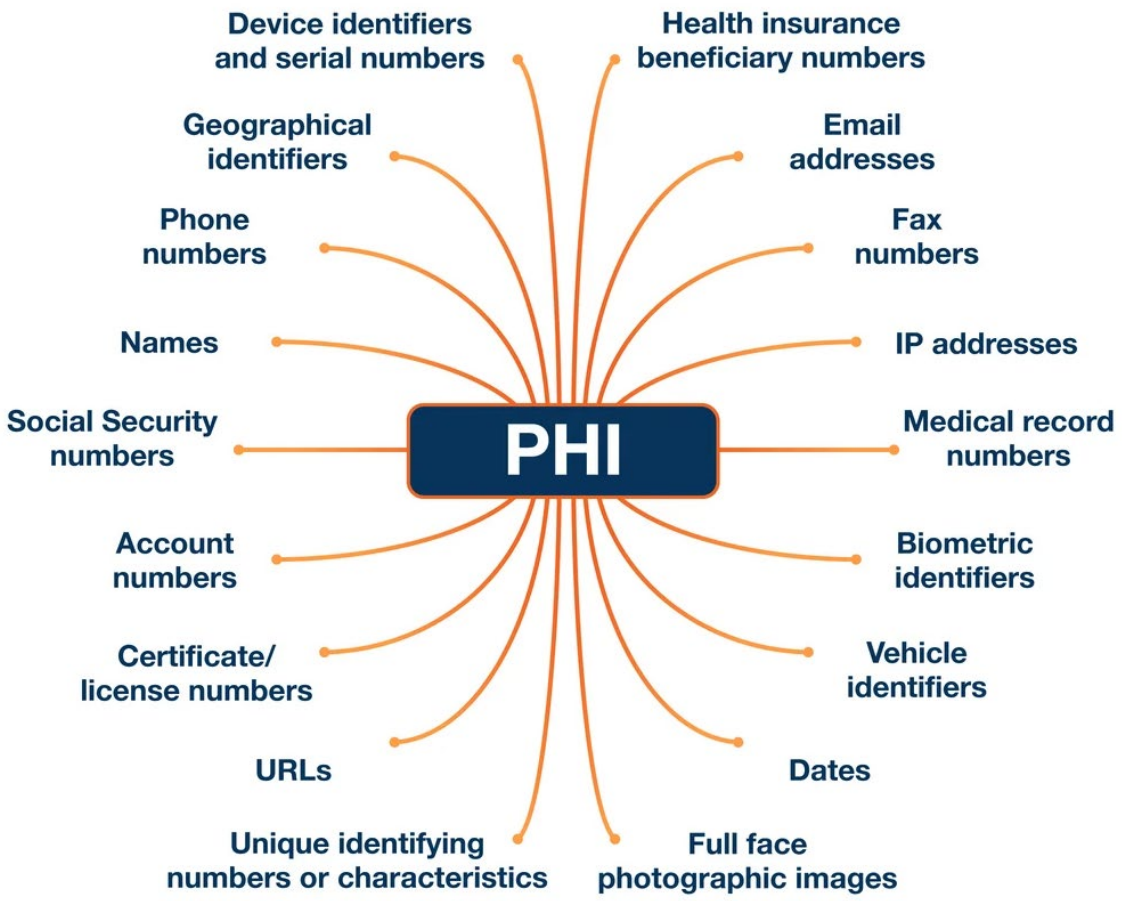
Operational continuity

Growing cyber threats in healthcare

Ethical and Moral Responsibility

What is Protected Health Information?

PHI stands for Protected Health Information, which refers to any individually identifiable health information that is created, received, maintained, or transmitted in the course of providing healthcare, health plan operations, or payment for healthcare.



HIPAA Privacy Rule

Limits use and disclosure of PHI

Patient rights regarding information

Minimum necessary standard

Requirements for healthcare organizations

A major goal of the Privacy Rule is to assure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well being. The Rule strikes a balance that permits important uses of information, while protecting the privacy of people who seek care and healing. Given that the health care marketplace is diverse, the Rule is designed to be flexible and comprehensive to cover the variety of uses and disclosures that need to be addressed.

HIPAA Security Rule

Administrative safeguards

Assigned Security POC, Workforce Security, Security Awareness Training, Contingency Planning, Security Incident Procedures, Business Associate Agreements

Physical safeguards

Facility Access and Control, Workstation Use and Security, Device and Media Controls

Technical safeguards

Access Control, Audit Controls, Authentication, Transmission Security

HIPAA Breach Notification Rule

Reporting timelines

Notification requirements

Breach assessment process

Consequences of delayed reporting

HIPAA Breach vs HIPAA Violation

Some sources conflate the terms violation and breach. It is important for Covered Entities and Business Associates to understand the difference between the two terms and what is considered a breach of HIPAA because, while HIPAA violations can be the *cause* of HIPAA breaches, only HIPAA breaches are reportable events.

Generally, a HIPAA violation is an event – or the lack of an event – that violates a HIPAA standard or implementation specification A HIPAA violation could be something relatively minor such as failing to implement physical safeguards to restrict workstation access to authorized users (which would be safe provided other safeguards are applied), or more serious – such as failing to respond to a patient access request in a timely manner.

A breach is “the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part [*the HIPAA Privacy Rule*] which compromises the security or privacy of the protected health information.”

Key healthcare data breach statistics for 2026

Breach frequency: incidents reported remain consistently high

Increase in ransomware attacks - Healthcare remains one of the most frequently targeted sectors because its systems are time-sensitive (clinical care), data-rich (identity, insurance, clinical history), and operationally complex (many vendors and integrations)

Attack types: hacking/IT incidents dominate, with email still a key entry point

Across healthcare reporting categories, “hacking/IT incident” classifications make up the largest share of large breaches, reflecting the shift from lost devices and paper records to network intrusions, credential theft, and cloud/service compromise. Email-based compromise continues to appear as a frequent initial vector, especially when multi-factor authentication (MFA) and conditional access controls are inconsistent.

Phishing and credential theft

Phishing remains a primary way attackers obtain access because it targets humans and workflows rather than a single server. In healthcare environments, the likelihood of a click is higher during high-tempo clinical operations, while inboxes are crowded with legitimate messages (referrals, lab results, imaging access links, portals, and vendor support threads).

Common Cybersecurity Threats for Tribal/Urban Health Clinics

Phishing and email scam susceptibility

Malware and ransomware

Unpatched or outdated software

Lack of or underutilization of Multi-Factor Authentication (MFA)

Unencrypted data storage and transmission

Inadequate access control policies

Medical Device Vulnerabilities

Business Associate Threats

Phishing Awareness

- Recognizing suspicious emails
- Avoiding malicious links
- Reporting phishing attempts
- Importance of staff training

Customer Service <customer.service@intranet-fi.com> 11:18 AM (23 minutes ago)

to me

Log in to Online or Mobile Banking to view your latest eStatement.

View as Web page Log in to Online Banking

CHASE

Date: 01/22/2021
Account Number ending in 8632

An ATM withdrawal or debit card purchase exceeds the amount you have chosen. To view more information on this transaction log in to Chase Online Banking or our U.S. Bank Mobile Banking website.

When you log in to view your statement, you can also view your most recent account activity, set up customized account alerts, update your contact information or ATM PIN number and more.

Please do not respond to this message. If you would like to contact us, please log in to Chase Online Banking and send a message to Customer Service.

You are receiving this email because you signed up for alerts through Chase Online Banking. If you no longer wish to receive this alert, log in to Chase Online Banking and go to My Alerts, select Account Alerts, and temporarily disable or delete this alert.

Chase Online Banking

Microsoft account unusual sign-in activity

S

support <info_support@lives-msn.com>
Sun 5/24/2020 9:39 AM
To: support

Your Microsoft account is about to expire due to inactivity

We want to inform you that the expiration date of your Microsoft e-mail account will be May 23, 2020.

When the expiration date has elapsed, the following services will be disabled:

- Sending and receiving messages
- Web applications that have been linked to your account

Simply click here and login into your Microsoft account and let us know that you are currently using this e-mail.

Thanks,
Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399, USA 2020 Microsoft Corporation. All

LogMeIn - Password Reset Inbox ×

LogMeIn <logmein@secure-monitor.com>
to me

3:11 PM (1 hour ago)

GoToMeeting

Was this you? Please confirm identity.

You received this email because someone requested a new password.

CREATE A PASSWORD

You will use your new password to log into:

- GoToMeeting

If you didn't make this request or need assistance, please Click Here

Ransomware Risks

Disruption of Patient Care

- Hospitals may lose access to electronic health records (EHRs)
- Delays in treatment, lab results, and medication administration
- Emergency services and surgeries may be interrupted

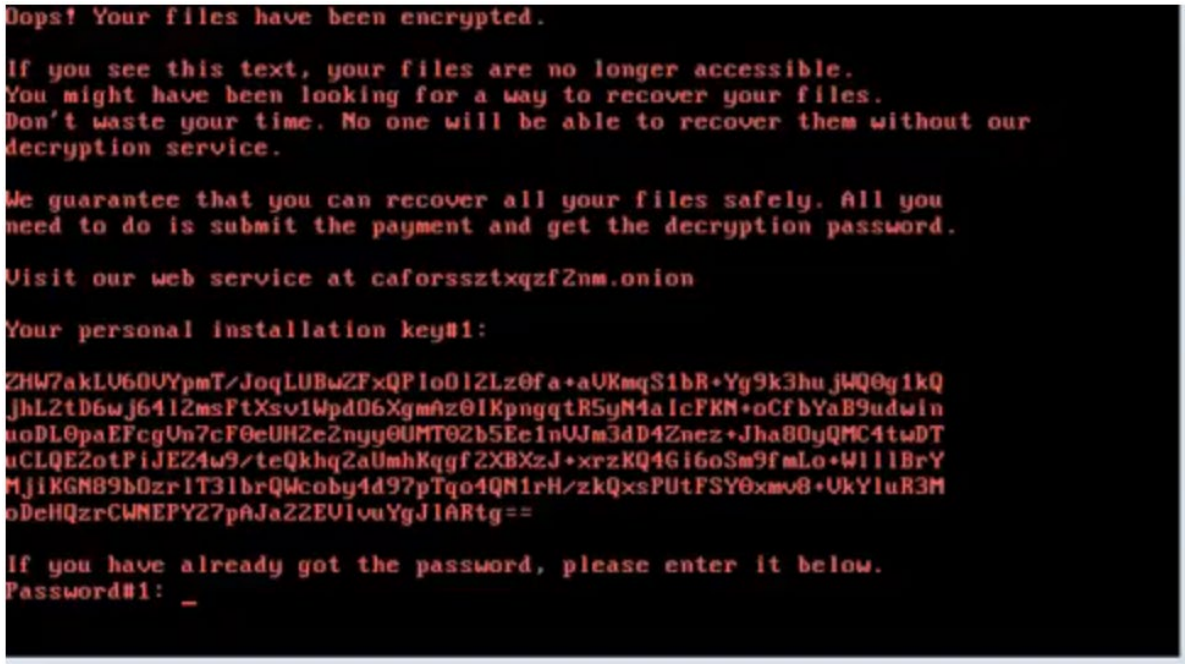
Loss of Access to Critical Data

- Patient records become encrypted and unusable
- Staff cannot retrieve medical histories or diagnostic information
- Communication systems may fail

Financial Losses

- Costs of system recovery and forensic investigations
- Potential ransom payments
- Revenue loss from downtime and canceled services
- Regulatory fines and legal expenses

Ransomware Risks



HIPAA and Compliance Violations

- Exposure of protected health information (PHI)
- Breach notification requirements
- Possible penalties for failing to safeguard patient data

Damage to Reputation and Trust

- Patients may lose confidence in the organization
- Negative media attention
- Long-term impact on community trust

Operational Downtime

- Scheduling, billing, and pharmacy systems may stop functioning
- Staff may need to revert to manual paper processes
- Productivity decreases significantly

Data Theft and Extortion

- Attackers may steal sensitive patient information
- Threats to publicly release data if ransom is not paid
- Increased risk of identity theft and fraud

Access Control Fundamentals

Role-based access control (RBAC) – Create access templates for specific jobs, and do not deviate from limitations. Create EHR roles that are based on benchmarked healthcare industry access.

Least privilege principle - Users receive only the minimum permissions needed for their job function. This limits the potential damage from compromised accounts and reduces opportunities for misuse.

Segregation of Duties - a core internal control principle that divides critical responsibilities among different individuals to reduce the risk of fraud, errors, and abuse.

- **43% of healthcare data breaches** involve insider access (Verizon 2024 Data Breach Investigations Report)
- The average healthcare worker has access to **over 1,000 patient records** they don't need for their job
- **58% of healthcare employees** admit to looking up patient records out of curiosity

Session management

Session management - is a critical technical safeguard under HIPAA's Security Rule to protect electronic protected health information (ePHI) from unauthorized access. Although the HIPAA law does not explicitly se the timeout period, it does require that "Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity".

1. Timeout Enforcement

Use **both idle and absolute timeouts**: idle limits protect when users step away; absolute limits cap total session length. Adjust durations based on workstation type (private office vs. shared kiosk) and ePHI sensitivity.

2. Give clear, accessible warnings

Display an inactivity warning before termination, with a visible countdown and accessible controls. Allow users to extend the session when appropriate or to save work and sign out. Support keyboard and assistive technology interactions and include optional audio cues in noisy clinical areas.

Multi-Factor Authentication (MFA)

- Additional layer of protection
- Reduces unauthorized access
- Common MFA methods
- Implementation considerations

Microsoft Authenticator

Clinical Workflow Challenges

Balancing efficiency with security in a clinic is mostly about reducing friction for staff while protecting patient data, systems, medications, and physical spaces. The best approach is usually "secure by default, easy in practice."

Here are the highest-impact areas to focus on:

➢**Simplify Authentication Instead of Weakening It**

Security often slows people down when login systems are clunky.

- Use **single sign-on (SSO)** so staff log in once for EHR, scheduling, labs, etc.
- Use **badge tap** or biometric logins in exam rooms.
- Set **fast session re-locks** with instant re-entry rather than forcing long passwords repeatedly.

Avoid: Shared logins, Sticky-note passwords, Turning off MFA because it feels inconvenient

Clinical Workflow Challenges

➢ **Design Workflows Around Clinical Reality**

If security policies fight the workflow, staff will bypass them.

- Place secure printers near nursing stations so PHI isn't left unattended.
- Use mobile workstations with auto-lock.
- Allow role-based access so staff only see what they need.
- Build emergency override procedures ("break glass access") for urgent care situations.

➢ **Automate Routine Security Tasks -** Automation improves both efficiency and protection.

- Automatic software patching
- Device encryption by default
- Scheduled backups
- Automated log monitoring
- Email phishing filtering
- Inventory tracking for devices and medications

Clinical Workflow Challenges

- **Train Staff in Micro-Learning Sessions -** Long annual compliance training is inefficient and poorly retained. More effective:
  - 5-minute monthly refreshers
  - Real-world phishing examples
  - Quick “security tip of the week”
- **Standardize Devices and Software -** Too many tools create both inefficiency and risk. Aim for:
  - Approved device list
  - Standard clinic laptops/tablets
  - Consistent communication platforms
  - Centralized device management

Standardization makes support faster and reduces configuration mistakes.

Third-Party and Vendor Risks

Third-party and vendor risks are the risks your clinic takes on when outside companies, contractors, or service providers have access to your systems, data, facilities, or operations.

In healthcare, vendors can include:

- Electronic Health Record (EHR) providers
- Billing companies
- IT support firms
- Cloud storage providers
- Telehealth platforms
- Medical device manufacturers
- Labs and pharmacies
- Cleaning, staffing, or transcription services

Even if the vendor causes the problem, your clinic may still face:

- HIPAA violations
- Operational disruptions
- Financial loss
- Patient safety issues
- Reputation damage

How to Reduce Third-Party and Vendor Risks

Before Signing a Vendor
Assess:
- Security practices
- HIPAA compliance
- Cyber insurance
- Financial stability
- Incident history
- Backup/recovery capabilities
- Request:
- SOC 2 reports
- Security questionnaires
- Penetration testing summaries
- References

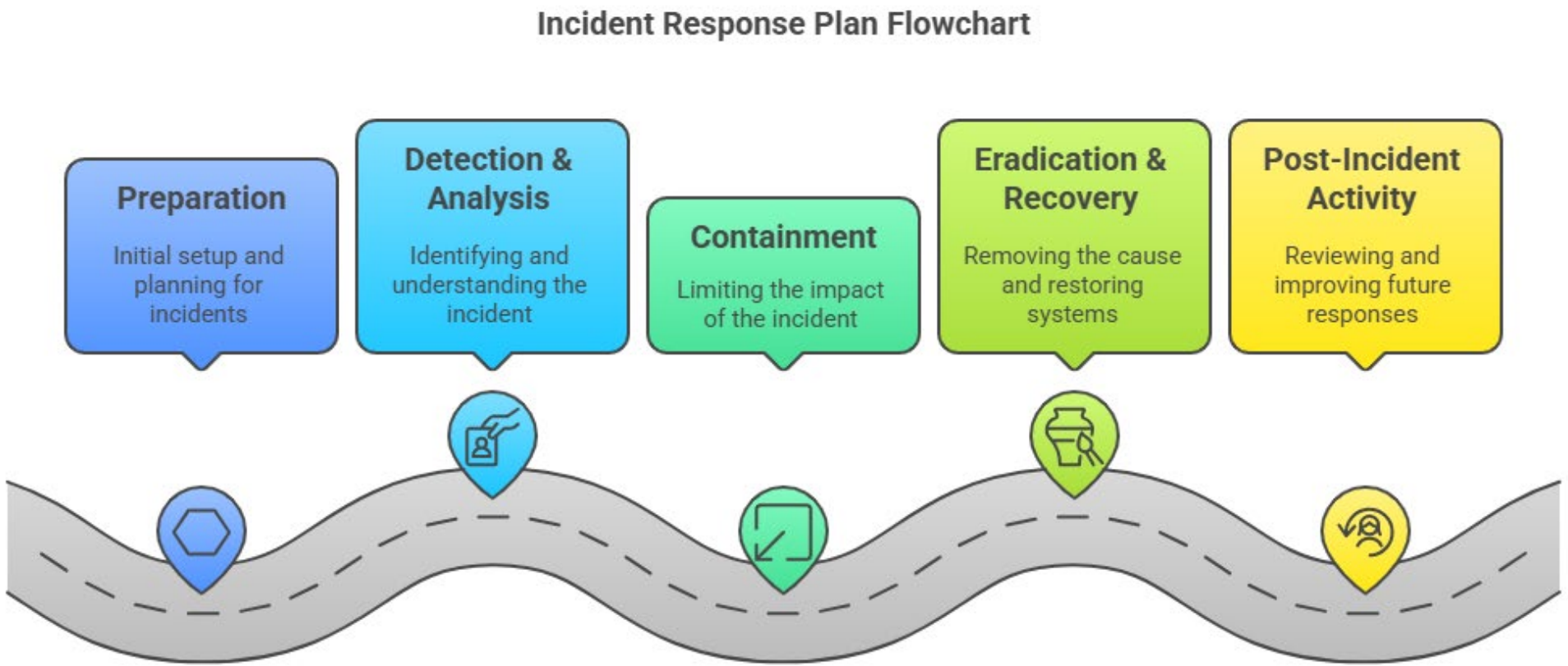
Contract Protections
Include:
Business Associate Agreement (BAA)
Breach notification timelines
Security requirements
Right-to-audit clauses
Data ownership terms
Exit/data return procedures

Limit Vendor Access
Use:
Least-privilege access
MFA
Time-limited accounts
Separate vendor accounts
Activity monitoring
Never give vendors shared staff credentials.

Monitor Vendors Continuously
Not just once during onboarding.
Track:
Security incidents
Expired certifications
Performance issues
Downtime frequency
Compliance updates

Have a Vendor Incident Plan
Know:
Who to contact
How systems will continue operating
Backup workflows

Incident Response Planning



Disaster Recovery and Backups

Key Components of Disaster Recovery

- ✓ **Data Backups:** Regular copies of important patient and organizational data are stored securely and are tested.
- ✓ **Recovery Plans:** Step-by-step procedures outline how systems will be restored after an incident.
- ✓ **Emergency Response Teams:** Assigned staff manage communication, technical recovery, and patient safety.
- ✓ **System Redundancy:** Backup servers or cloud systems help maintain operations if primary systems fail.
- ✓ **Testing and Drills:** Organizations regularly test recovery procedures to ensure readiness.

Privacy Compliance Documentation

- **Notice of Privacy Practices (NPP)** This is a document given to patients explaining:
  - How their PHI is used
  - Their privacy rights
  - How to file complaints
- **HIPAA Training Records** Documentation proving employees completed required training. Includes:
  - Training dates
  - Attendance logs
  - Topics covered
  - Signed acknowledgments
- **Patient Authorization Forms** Signed forms allowing disclosure of PHI. Examples:
  - Medical records release
  - Research authorization
  - Marketing consent

Retention is important for audits.

Case Study: California IHS Clinics Data Breach Scenario

Overview of breach – In November 2025, 2 California IHS Clinic systems were hit with ransomware, affecting 15 locations

Root cause analysis – Investigation revealed lack of Multi-Factor Authentication, unsecure administrator accounts. Initial breach came through e-mail, likely months before the cyberattack. A service account with full admin privileges was leveraged due to unencrypted configuration file with password in plain text. The attackers used compromised credentials to move laterally across each domain and spread the malware from one IHS clinic to another.

Preventive measures:

Implement MFA

Train staff on phishing emails

Store passwords/configuration details in encrypted files

Building a Culture of Security

Leadership Must Model Security Behavior Culture starts with leadership.

If managers:

- Share passwords
- Ignore MFA
- Bypass procedures
- Delay updates

…staff will do the same.

Leaders should:

Follow the same policies as everyone else

Complete training visibly

Report suspicious activity

Support security investments

Avoid blaming employees for honest mistakes

Building a Culture of Security

Encourage Reporting Without Punishment

Staff should feel safe reporting:

- Suspicious emails
- Lost devices
- Wrong-recipient faxes/emails
- Privacy mistakes
- System abnormalities

If employees fear punishment, incidents get hidden.

Focus on:

- Early reporting
- Fast containment
- Learning and improvement

Reserve disciplinary action for intentional or repeated negligence.

Key Takeaways

Protecting ePHI requires ongoing effort

Security must align with patient care

Compliance is everyone's responsibility

Preparedness reduces risk

Questions?

Reese Weber, MBA, CISSP

Chief Information Security Officer and Privacy Coordinator

Indian Health Service, California Area

916-930-3981 x 307

Theresa.weber@ihs.gov

https://www.linkedin.com/in/reese-weber-mba-cissp-6085203b

References:

History of Risk https://risksciences.com/history-of-risk/

Summary of the HIPAA Privacy Rule Microsoft Word - MO02PBf_pdf.rtf

2025 Health Sector Cyber Threat Landscape- Health-ISAC_2025-Annual-Threat-Report.pdf

HIPAA Basics for Providers: Privacy, Security, & Breach Notification Rules

HHS HIPAA Security Risk Assessment Tool - https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool

HHS / HealthIT.GOV SRA User Guide- https://www.healthit.gov/sites/default/files/page/2019-10/SRATv3.1User%20Guide.pdf

Role-Based Access Control (RBAC) Implementation Guide | IBM


INDIAN HEALTH SERVICE
PHS · 1955 ·