OSP

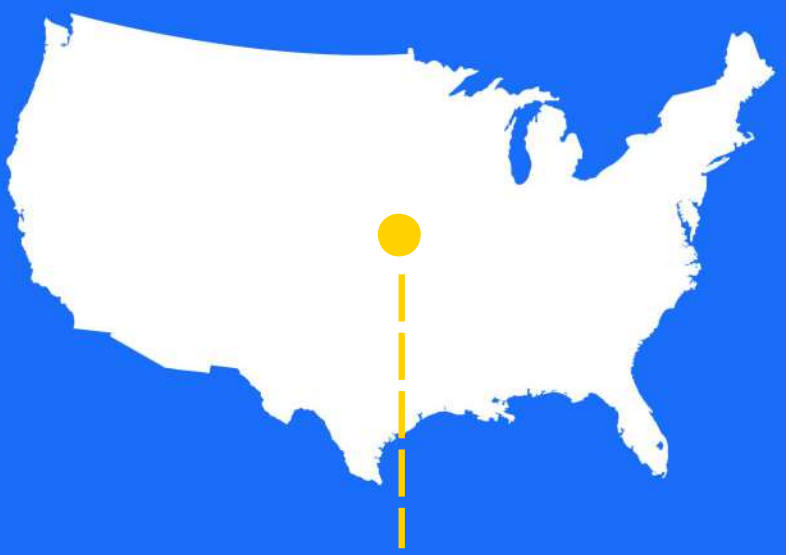
THE STEP-BY-STEP TECHNICAL GUIDE TO MEET HIPAA COMPLIANCE

A guide to help healthcare software developers to understand the HIPAA Security Rule

Table of Contents

1 Introduction

15,085,302 patient records were breached in 2018. - Protenus' 2019's Annual Breach Barometer Report



That equates to more than 4.5% of the population of the US

"I know HIPAA compliance is important, I just don't know how to maintain HIPAA Compliance?"

This statement sounds quite familiar to healthcare professionals. Unfortunately, noncompliance with the HIPAA regulations puts organizations at greater risk of a data breach now than ever before.

Endorsed in 1996, the Health Insurance Portability and Accountability Act (HIPAA) is a law that implements data privacy and security provisions for safeguarding medical data. Essentially, if you're handling, transmitting, in possession of, or responsible for any medical records; you should be in compliance with HIPAA.

Did you know that there are stiff penalties and fines for a violation? A data breach can put you at the risk of heavy fines and penalties and cause a dent on your credibility within the healthcare community.

2 HIPAA Facts

1 in 7 Healthcare Organizations
have still not appointed a HIPAA compliance officer

80% of Healthcare Organizations
fail meaningful use audits

1 in 4 HIPAA breaches
still not reported

Unauthorized access to records
accounts for 20% of HIPAA breaches

50% of Healthcare Organizations
believe they would fail a HIPAA Audit

Phishing and Ransomware
the top hacker tactic

Average Cost
per record is $363

Ransomware
for medical records accelerating rapidly

About 600 HIPAA Violations
referred to DoJ

Nearly 200 million
patient records compromized since introduction of HIPAA

3 The Need for 100% HIPAA Compliance

- Fosters a culture of compliance throughout the organization
- Ensures the privacy and security of patients data
- Promotes careful handling of PHI to improve patient satisfaction
- Eliminates the legal risk by sharing PHI in accordance with HIPAA
- Reduces executive and organizational liability
- Protects the organization and staff from personal liability
- Helps build a foundation for future technology implementations
- Helps to avoid expensive add-on security measures

5 Major HIPAA Components

HIPAA Privacy Rule

PHI Disclosure Rules

HIPAA Security Rule

Standard to Safeguard ePHI

Omnibus Rule

Merges HITECH rules into HIPAA

Breach Notification Rule

60 Days to notify HHS

Enforcement Rule

How investigation are conducted

4 Checklist: HIPAA Web App Security

A. DATA GATHERING

1. Evaluate the rendered site
   - Use a spider to mine your data and check for any missing elements
   - Check for data leakage via web server metafiles. Ex. .DS Store, robots.txt, sitemap.xml
   - Check the caches prominent engines to verify the accessibility
   - Verify the webpage metadata and comments to avoid data leakage

2. Development Evaluation
   - Verify the application design framework
   - Check the leveraged technologies
   - Assess user roles
   - Determine the points of entry
   - Be careful of client-side scripts
   - Determine all delivery channels like a mobile app, mobile web, and web

3. Platform and Hosting Assessment
   - Manage any content that is provided by independent parties
   - Evaluate all the used ports and hostnames
   - Figure out the co-hosted applications
   - Verify all web services system

The Types of Injections to Be Tested

- SQL
- HTML
- XML
- XXE
- SSI
- XQuery
- IMAP/SMTP
- Code
- LDAP
- ORM
- XPath
- NoSQL
- Command
- Expression Language

> **"Truly understanding risk management is much more important than compliance."**
>
> **- Andrew Hicks**
> National Healthcare Practice Director

B. MANAGE CONFIGURATION

- See what administrative or application URLs might be implemented that are too common to be secure
- See what files are unreferenced, old, or backups
- Verify all supported HTTP techniques plus prevent the Cross-Site Tracing (XST)
- Verify the file extensions processing
- Control rich internet application (RIA) cross-domain access
- Verify the secure HTTP headers in place
- Manage any confidential data like login credentials or API keys, within the client-side script

C. CONFIRM TRANSMISSION SECURITY

1. Encryption and Protocols
   - Check the key length, SSL version, and the used algorithms
   - Confirm that you have valid digital certificates
   - Validate the HTTPS is leveraged any time when usernames or passwords are sent
   - Make sure that HTTPS is executed throughout the application
   - Confirm that HTTPS is in position for all session tokens' delivery
   - Check the HTTP Strict Transport Security (HSTS) implementation
   - Verify HTML5 web messaging
   - Confirm the use of CORS

2. Representational state transfer (REST) and web services
   - Evaluate REST implementation
   - Check for any issues with web services

D. VERIFY AUTHENTICATION

1. Determine the functionality of the app password
   - Cross-verify the password quality rules
   - Test the working of 'Remember me'
   - Check that recovery, reset and change the password options function correctly
   - Ensure the consistency of application authentication with alternative channels and shared authentication schema/SSO

2. Functionality Concerns with Authentication
   - Check to see if nefarious parties can successfully identify users
   - Determine if authentication bypass can happen
   - Verify your defences against brute force attacks
   - Confirm the functionality of encryption on credentialing channels
   - Verify HTTP cache Management (like Expires, Max-age, and

Pragma)
- Maintain the fitting working order of user-accessible authentication history

E. MANAGE THE SESSION

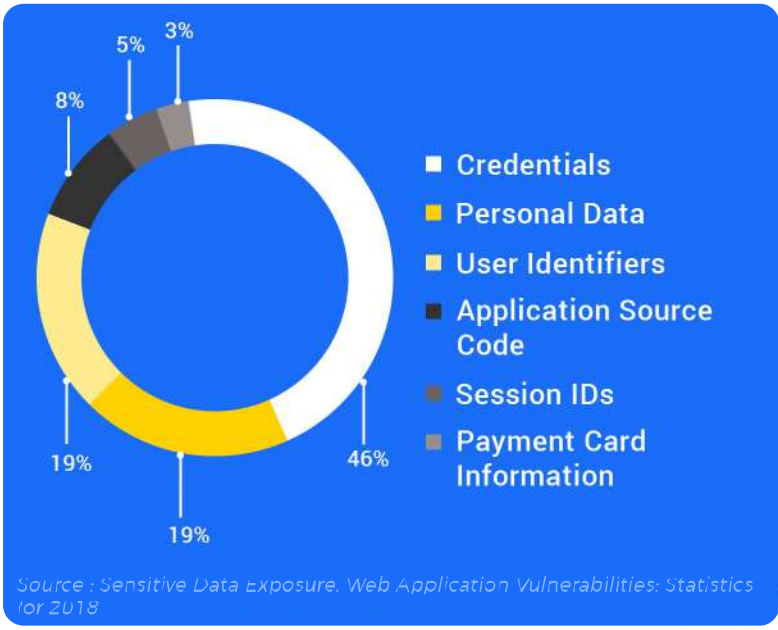
- Verify the working of tokens in cookies, token in URL or other session management method
- Check for cookie flags with session tokens (both HTTP and secure)
- Confirm the expiration related to the duration of the session cookies
- Determine that session termination occurs, following a maximum lifetime
- Following a relative timeout and log out, confirm that the session terminates
- Check if it is possible to start more than one synchronous session per user
- Validate the login, log out, role changes, a new session token is generated
- Verify the consistent application of session management during the shared session management
- Determine the session puzzling
- Ensure protection from cross-site request forgery (CSRF) and clickjacking

F. VERIFY THE AUTHORIZATION

- Review the path traversal
- Assess the system for possible missing authorization
- Validate if insecure direct object references are occurring
- See if privilege escalation is present
- Check any possible issues with horizontal access control

G. VALIDATE YOUR CRYPTOGRAPHY

- Assess the possibility of weak algorithms
- Check the correct usage of algorithms based on the relevant context
- Evaluate the randomness functions within the system
- Verify the occurrence of salting as planned
- Check the credibility of encryption



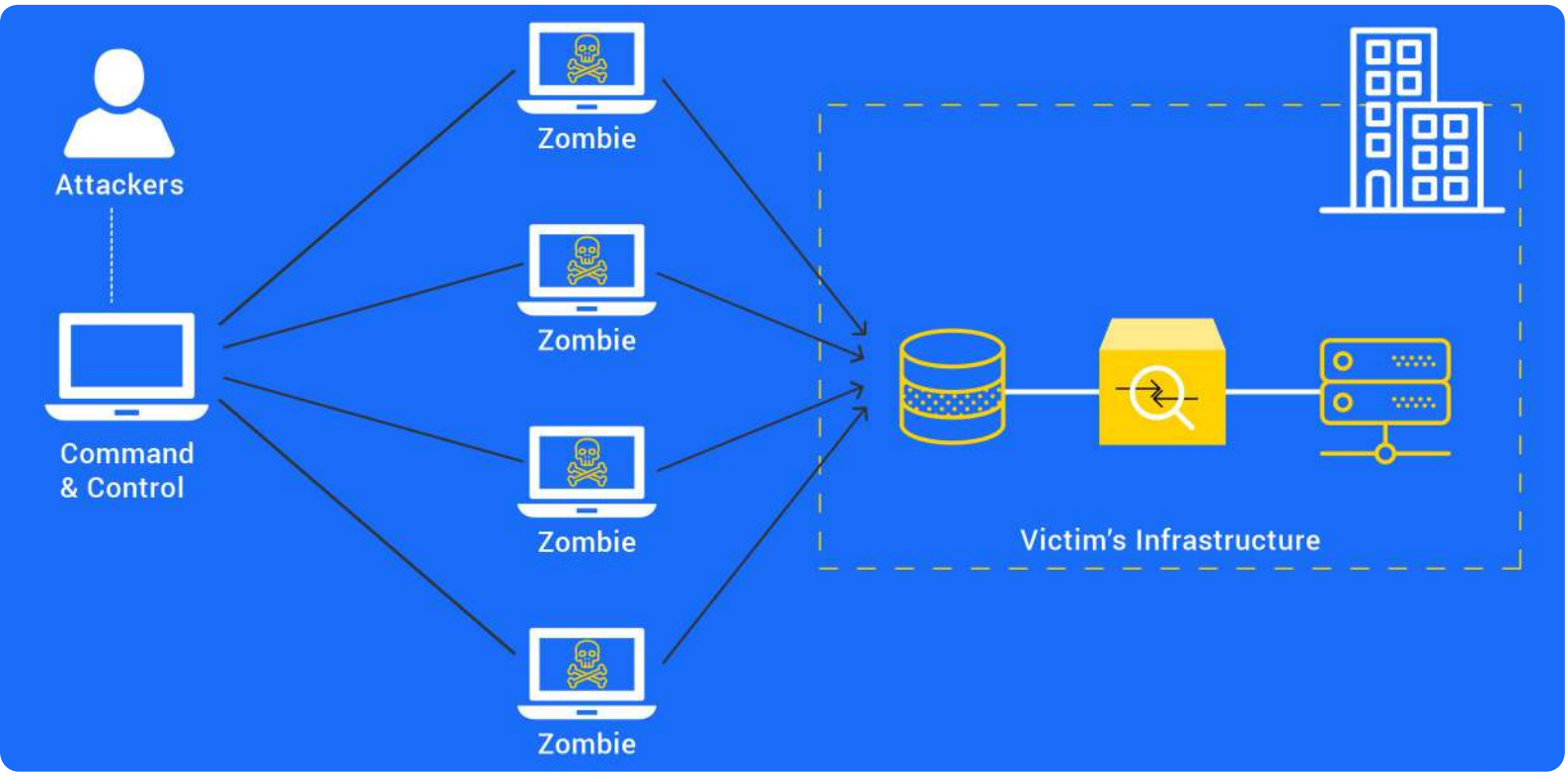
Source : Sensitive Data Exposure, Web Application Vulnerabilities: Statistics for 2018

Additional Data Validation Tests

- Cross-site scripting
- The occurrence of stored cross-site scripting
- DOM-based cross-site scripting
- Cross-site flashing
- Presence of overflow
- Verify format string issues
- Possible incubated weaknesses
- Smuggling or splitting of HTTP
- Verb tampering with the HTTP
- Possible open redirection
- Remote file inclusion
- Local file inclusion
- Consistency of validation rules for the server-side and client-side
- Parameter pollution with HTTP
- Auto-binding
- Mass Assignment
- The functioning of NULL/Invalid Session Cookie
- The quality of data integrity
- Protection against the misuse of the application
- Process timing for consistency
- Web storage SQL injection
- Offline functioning of the application

Verify Denial of Service (DoS) Concerns

- Assess the system for anti-automation
- Verify the working of account lockout
- Verify that SQL wildcard DoS is not present
- Ensure the vulnerability of the system to HTTP protocol DoS



5 Cloud Strategy

Can Cloud Hosting be HIPAA-compliant?

Though there is plenty of paranoia about HIPAA-compliant cloud hosting, it can be made possible not only to secure the IT systems but also to deliver the critical systems seamlessly.

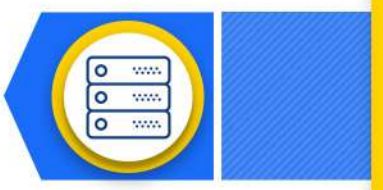
Must have HIPAA-compliant Cloud Features

- Firewall and Intrusion Prevention System
- Fully encrypted Virtual Private Network
- Robust Log Management
- Backups and Data Recovery
- High Availability & Reliability
- SSAE 18 Certification
- Third-Party HIPAA/HITECH Auditing

Quick Checklist for HIPAA-compliant Cloud Hosting

- Get complete data security, data management, and training procedures on file
- Build a system of developing unique user IDs and passwords and modes for login, logout, decryption as well as emergencies
- Build strategies to manage access to E-Systems containing PHI
- Defined rules to store, transfer, trashing and reimplementation of healthcare data
- Audits and logs of system usage for SSAE 18 and SOC audited infrastructure
- Guidelines for hosted data transfer in every scenario. Ex. cloud, email, etc.
- Smart quality control policies for all forms of hosted data
- Verify the availability of dynamic data
- Maintenance of distinction in servers hosting web, database, and production
- Antivirus and Multifactor Authentication
- Operating System (OS) patching management
- Evaluation of private IP addresses and private hosted environment
- Build disaster recovery and backup strategies
- Implement encrypted VPNs and private firewalls

6 HIPAA-Compliant Hosting Checklist



Private Hosted Environment

Hosting data, applications, and backups exclusively for one organization in a private cloud.

SSAE Certification

Certification to confirm an organization meeting an auditing standard for service organizations, superseding Statement on Auditing Standards no. 70 (SAS 70).

Business Associate's Agreement

A business contract between healthcare stakeholder (provider, payer or clearinghouse) and a business associate.

Multifactor Authentication

A security system with multiple methods of authentication from independent categories of credentials to verify the user's identity.

Firewall

A network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

Offsite Backups

A method of backing up data to a remote server or to media that is transported off-site.

Encrypted VPNs

A virtual private network that helps you safely connect any two machines leveraging advanced protocols such as IPsec and GRE.

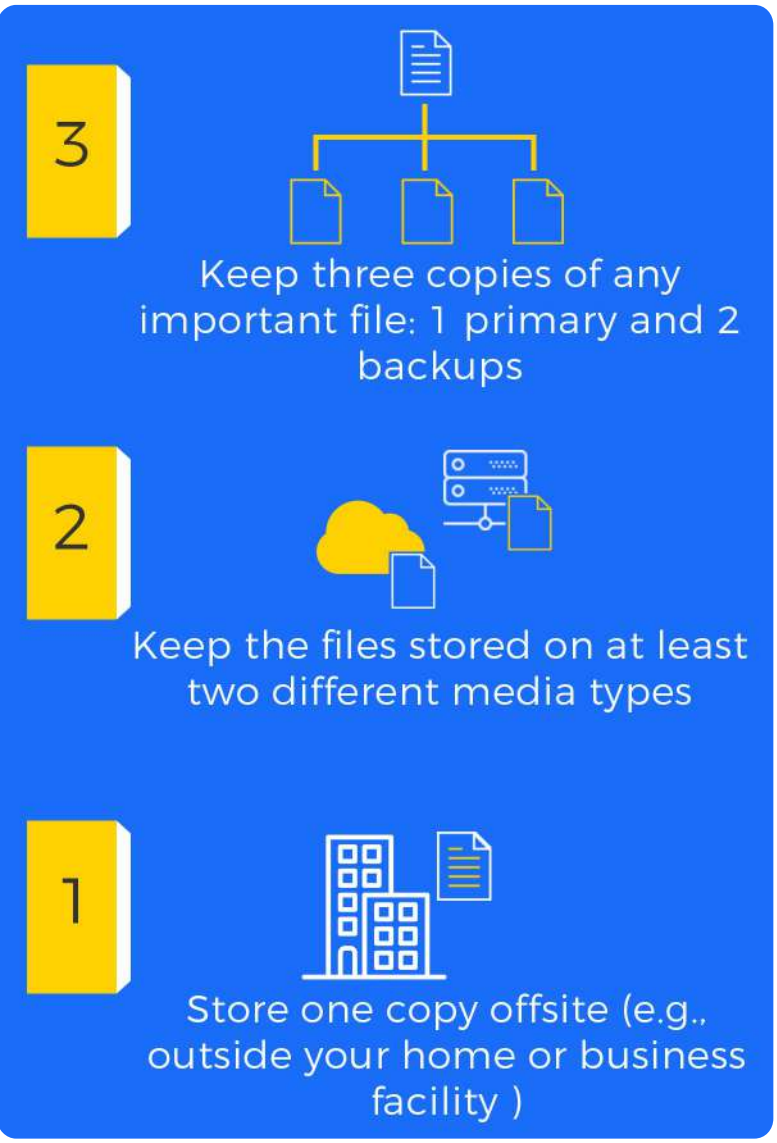
SSL Certificate & SSL VPN

An SSL Certificate encrypts data, populates HTTPs Protocol and a lock icon, and validates the site and its ownership.
An SSL VPN is a virtual private network that uses secure sockets layer technology to encrypt connections through a web browser.

7 Disaster Recovery Plan

The Must-have Components in HIPAA Disaster Recovery Plan

- To minimize interruptions to the normal operations
- To limit the extent of disruption and damage
- To minimize the economic impact of the interruption
- To establish alternative means of operation in advance
- To train personnel with emergency procedures
- To provide for smooth and rapid restoration of service



1. Inventory all physical and digital assets

- Update lists of all hardware, software, data, and security certificates
- Maintain a list of cybersecurity applications, certificates, extensions, and other cyber protection methods
- Break down the data into separate lists such as tangible vs intangible assets for a simplified structure

2. Have a data backup strategy and perform data restoration tests

- Back up your data and test to ensure the restoration methods work
- Test your data backups regularly to ensure they are in good condition and are reliable

3. List of all personnel and their DR responsibilities

4. Develop a comprehensive communications plan

- Build a communications plan including alternative communication methods of communication

- Implement preventive measures for your network by leveraging network path diversity or using ad hoc networks

5. Outline alternative work capabilities and redundancies

- Establish alternative options for your IT infrastructure, hardware, software, IT security, and communications capabilities

6. Outline how sensitive data should be handled

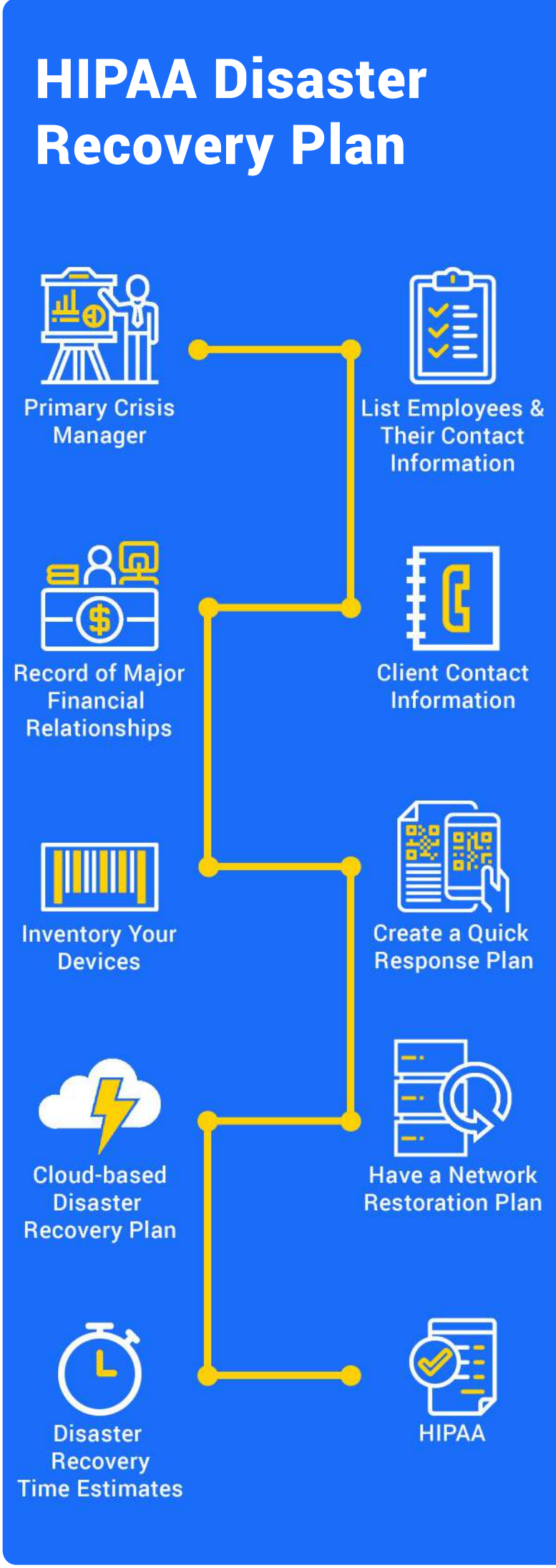
7. Ensure disaster recovery information is included in SLAs

- Review the service level agreements (SLAs) you have with all third-party vendors especially your backup data providers and peer agencies

8. Keep your information up to date

9. Test your plan and procedures regularly and conduct exercises

10. A data recovery plan should include the following things

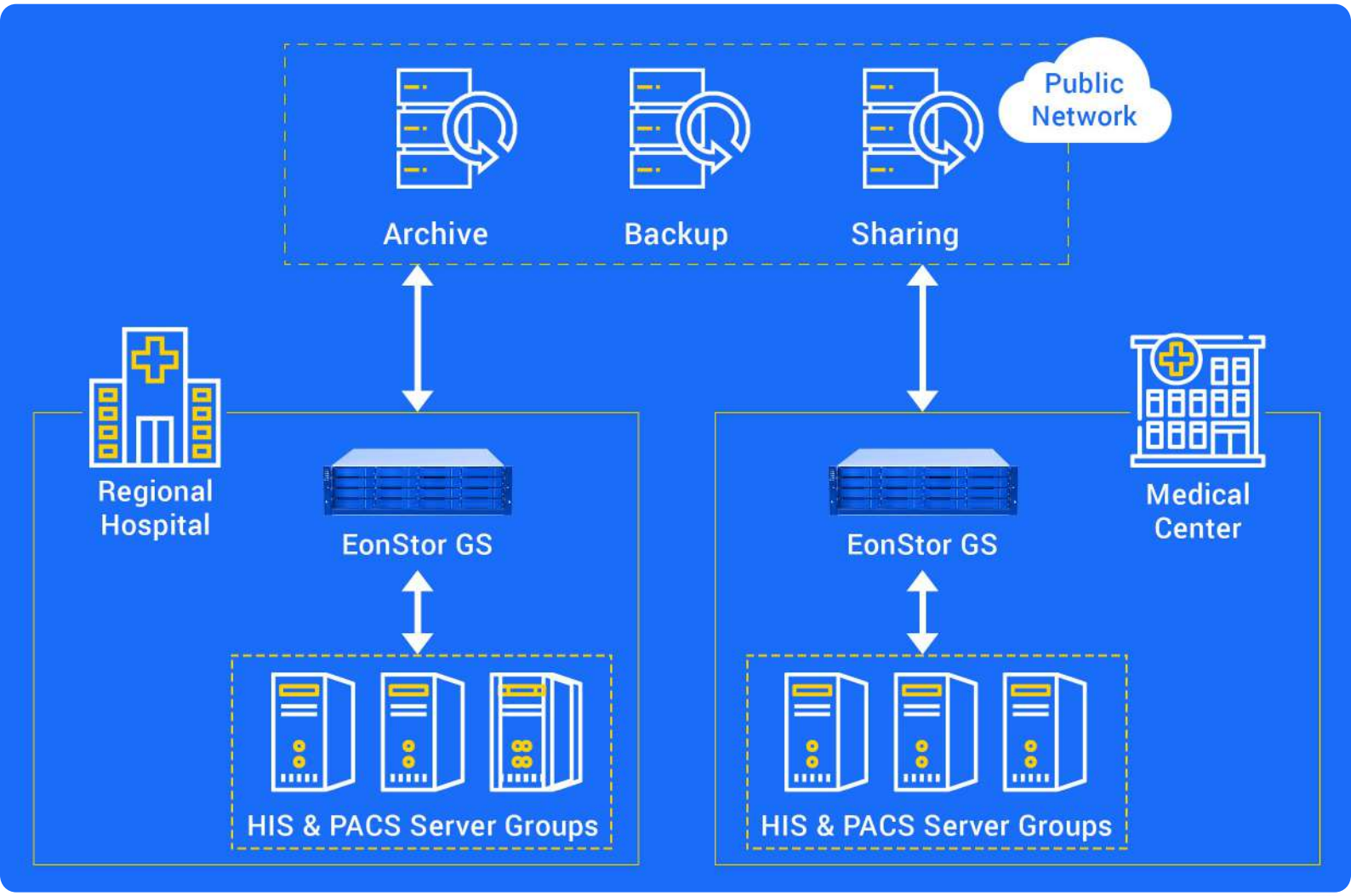


8 Storage Backup Plan

The primary objective of HIPAA is to protect patient privacy, so keeping this identifying health data private and secure is the principal goal of storage.

How to Remain Compliant When Using or Collecting HIPAA Protected-Data

- Notify the user of your data policies
- Protect the health-related data strong user authentication methods
- Encrypt the data where it is stored, as well as during the transmission
- Provide a way to remove the sensitive PHI if the device is lost or stolen
- Enable strong firewall protection
- Protect the data with anti-malware software with regular updates
- Develop a system to notify users and the U.S. Department of Health and Human Services if the data is breached

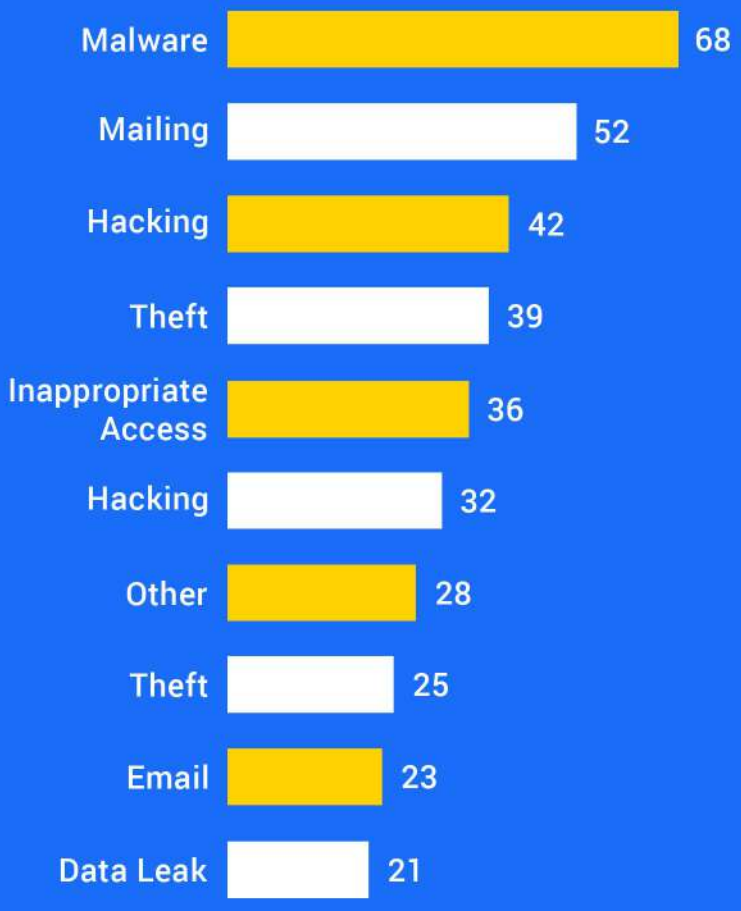


PHI Storage Best Practices

PHI must meet certain Technical, Administrative and Physical safeguards during storage and transmission in order to be HIPAA-compliant. They are,

1. Administrative Best Practices
2. Physical Best Practices
3. Technical Best Practices

Most Common Types of Data Breach



Technical Best Practices

- ePHI is protected from unauthorized and malicious access during transit and storing to the cloud
- Build a plan for end-to-end medical data encryption
- Data should be backed up to the cloud with a provider who offers unlimited previous file version histories
- Intrusion detection and alarm systems
- Environmental controls, fire detection, and suppression systems
- Appropriate security for electronic data, such as encryption, authentication, and passwords
- Remove redundant infrastructure for data centres
- Duplicate copies of data for disaster recovery purposes
- Data integrity inspections to detect file corruption
- Dedicated resources to monitor protection systems
- Special management of archived data and disaster recovery

Biggest threats to data security : Employee Negligence

Employee behaviour (a combination of mistakes, lax access controls, and malicious activity)

Unintended mistakes by internal staff (making this the leading overall cause of data breaches)

Source : Axway Infographic : The Road to HIPAA Compliance

By 2016,

80%

of reported security failures will be due to:

Lack of Risk Assessments

Poor Governance

Source : "Leading Cause of Data Security Breaches Are Due to Insiders, Not Outsiders." PR Newswire

Migration to EHR

- Centralized location or trusted vendor for storage of EHR records and conversion services
- Full disaster recovery backup of all records at a separate location

Information Destruction

- Retention schedules that include federal and state regulations
- Consistent information disposal policies and procedures
- Audit trail and documentation to destroy electronic materials to a nonrecoverable form
- Secure chain of custody if the data is transported for destruction
- Secure destruction of electronic records in accordance with retention policies

9 QA Test Strategies

For 100% HIPAA-compliant systems, well-defined QA testing strategies play a vital role. HIPAA testing strategies include the following components,

1. Primary Sanity Testing
2. Development of Roles Matrics
3. Full-feature Testing

A. Primary Sanity Testing

Primary sanity testing is highly essential to detect major bugs hindering HIPPA compliance. Here are the primary sanity testing components,

1. Verify for a High-risk Role

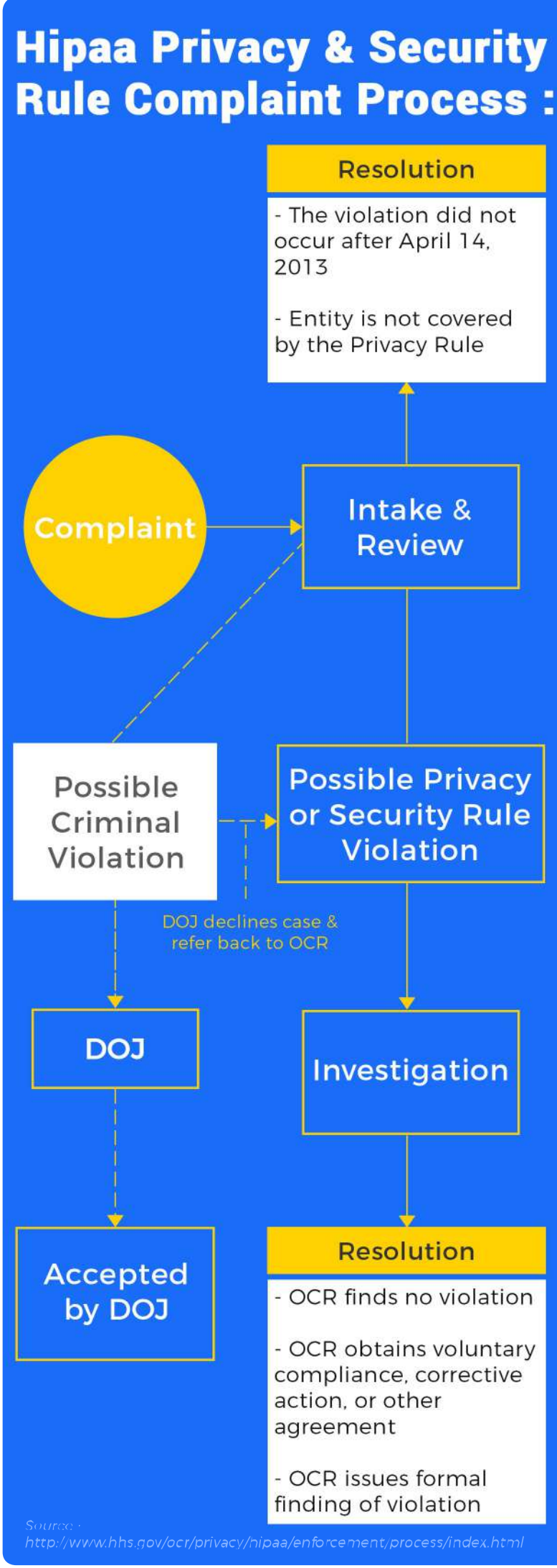
- User can authenticate successfully and is granted all the access
- Each action is properly tracked and recorded in detail

2. Evaluate Encryption

- Electronic Protected Health Information (EPHI)
- Audit trail entries

B. Roles Metrics

- Identify all the roles in the system and their access level to all the components of the application
- Determine the risk level associated with each role/ component/operation relationship



> **“Cybersecurity is a shared responsibility, and it boils down to this : in cybersecurity, the more systems we secure, the more secure we all are.”**
>
> **-Jeh Johnson**
> Former United States Secretary of Homeland Security

C. Full-feature Testing

1. User authentication
   - Ownership-based: ID cards
   - Knowledge-based: User ID/Password
   - Biometric based: Fingerprint
   - Login failure for: Empty & invalid user ID/empty & invalid password/expired account, etc.
   - Locked-out account
   - Login success after password change
   - Characteristics of password change itself
   - Login idle timeout
   - Login credentials

2. Information disclosure
   - Role-based access (RBA)
   - Patient allocation (PA)

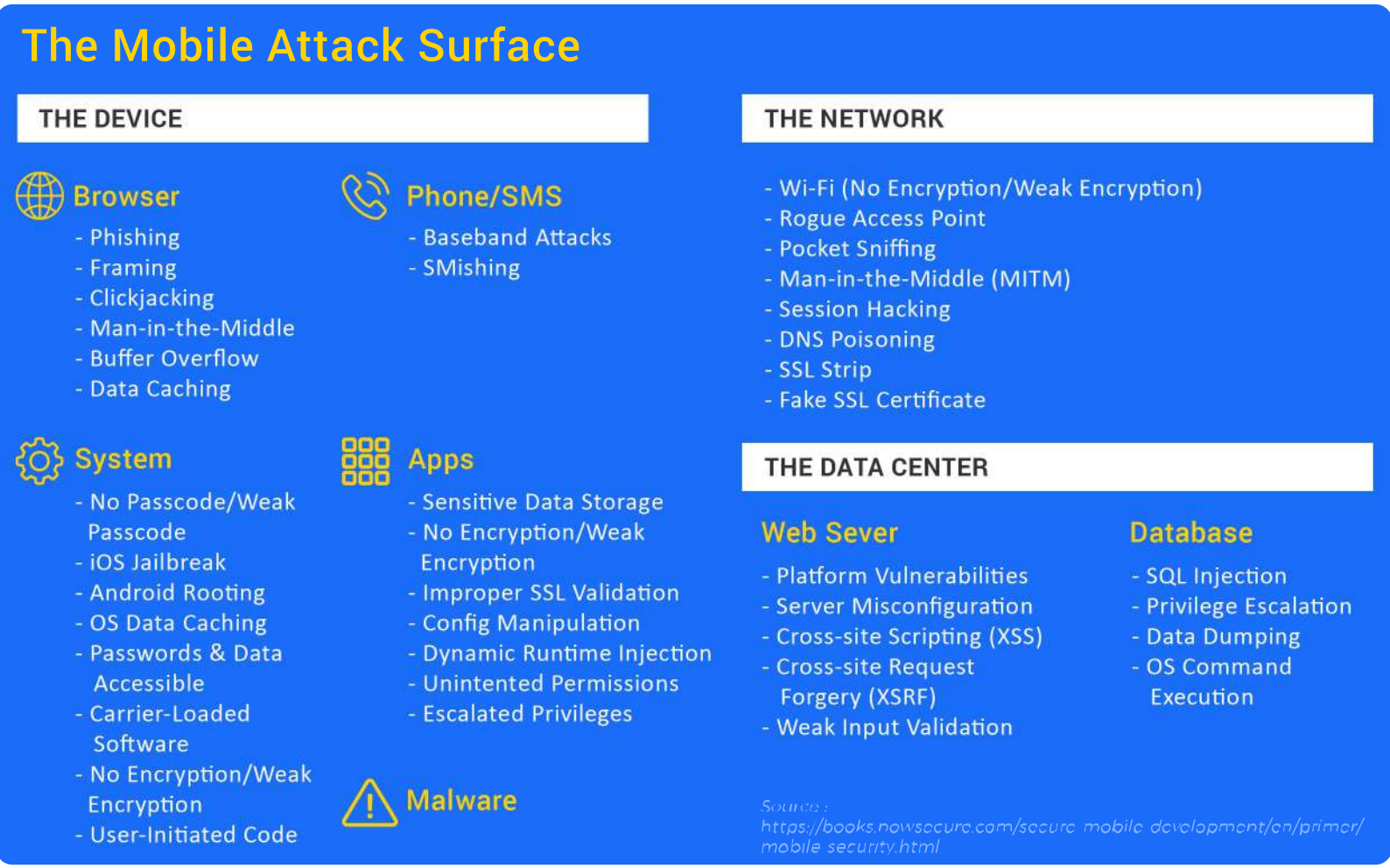
3. Audit trail
   - That all expected audit trail entries exist
   - That each audit trail entry contains date and timestamp of the action, user ID, etc.
   - Entries conform to the software clarity requirements
   - All attempts to breach security are recorded
   - Audit trail is encrypted

4. Data transfers
   - Data access between all workstations and mobile devices
   - Data transfer to an external location
   - The movement of data to an offline storage

5. Information on correct data use
   - Verify that the application provides an explanation of correct data use prior to access
   - Test of a training version of the application that allows users to see the working of the application before granting access to real EPHI

10 Mobile App Compliance

The Mobile Attack Surface



Challenges Faced by mHealth App Developers

- The Line of Action
- Other HIPAA Security Rules & Their Proper Compliance
- Push Notifications
- Messaging Violations
- Continuous, Stringent, Full FDA Approval on All Ends
- Mobile Security

How to Make Your Mobile App HIPAA Compliant?

- Unique User Authentication
- Encryption of Data
- Automatic Logoff
- Remote Wipe
- Regular Updates
- Audit Logging
- Backup and Syncing

1. Manage all devices:

Security settings and configurations must be constantly maintained.

2. Enable remote lock and wipe:

An unauthorized user should not be able to access data on a misplaced device.

3. Enforce data encryption:

Full device or app-by-app encryption must be monitored and enforced.

4. Enforce password:

Enforcement of a device-level password to prevent unauthorized data access.

5. Monitor OS integrity:

Avoid the device's operating system to get compromised, Ex. jailbroken or rooted.

6. Implement the auto-wipe policy:

To minimize the risk of brute force attacks on lost devices, by wiping the device after a number of failed password attempts.

7. Secure email and attachments:

Prevent corporate email from being forwarded through a personal account. Create a policy to protect attachments from being accessed by untrusted file readers.

8. Control file sharing:

Prevent untrusted file-sharing apps from gaining access to secure medical data distributed through email or SharePoint.

9. Track devices:

Enabling or disabling location tracking are controlled through extensive privacy policies, that ensure the consistency of administrator actions with corporate privacy standards.

10. Quarantine non-compliant devices:

Automate compliance actions, such as quarantine and selective data wipe to ensure data security.

11. Log devices and actions for audit:

Create audit logs for compliance to maintain device management information about the device and unauthorized device activities.

11 HIPAA Cheat Sheet

SECURITY RULES :

TECHNICAL SAFEGUARDS

Access Control

- Unique identifier required to determine user identity in electronic records
- Emergency procedure required for obtaining electronic PHI (ePHI) during an emergency
- Automatic logoff that terminates an electronic session after a time of inactivity
- Encryption and decryption of ePHI

Integrity

- Implement mechanisms to authenticate validity of ePHI
- Ensure access to ePHI is the one claimed
- Ensure that electronically transmitted ePHI is encrypted and is not improperly modified without detection

PHYSICAL SAFEGUARDS

Facility Access Control

Workstation Use

Workstation Security

Device & Media

ADMINISTRATIVE SAFEGUARDS

Security Management

Workframe

Incident

Contingency

PRIVACY RULE :

- Disallow impermissible use and disclosure of PHI
- Notify covered entity of breaches
- Provide covered entity (or individual) access to PHI
- Discloses PHI to Secretary of Health and Human Services (HSS) when asked
- Document and account for all disclosures of PHI

12 Summary

Whatever the size of an organization, the cost of a data breach will prove more expensive than the costs of building strong HIPAA-compliant system infrastructure. Taking a proactive approach will help developers program a full-proof software system that, can avoid most threats and keep company operations running smoothly.

Being 100% HIPAA requires,

- Create internal HIPAA policies that help your staff understand the importance of security
- Stay current with security updates to keep up with threats that constantly evolve
- Build a strong risk assessment policy involving every channel, every person, all systems that are interacting with your ePHI data
- Prioritize security efforts and execute effective countermeasures to mitigate the risks

OSP

We are a leading software development company aiming to empower, and inspire the world with next-gen solutions. We help in simplifing every step of the development process, from system architecture design to quality delivery. Our intelligent processes enable quick deployment of enterprise-grade solutions against the toughest, and most complex challenges.

We are re-imagining how technology can empower Healthcare, AI, Analytics, and Financial organizations to build solutions for every day use in business applications.

With 10+ years of experience, and 200+ customers worldwide, we're leveraging technology to build the future today.

---

www.osplabs.com

Discuss Your Project

solutions@osplabs.com

Texas | California | Maryland | Mumbai

© 2019