Information Security Policy Document

Tristen Woodruff, Soumya Konar

Table of Contents

**Introduction1**

Purpose3

Scope3

**Information Assets4**

Patient Information4

Employee Information5

Organizational Information5

Greatest Threats6

Likely Threat Actors6

**Hardware and Software7**

Database Management System and Security7

Development Programming Languages7

Firewall7

**Liabilities7**

**Roles and Responsibilities8**

**Policies9**

**Standards14**

**Practices14**

**Programs15**

**Incident Response17**

**Future Review18**

**References20**

1. Introduction
   1. Purpose

This document’s purpose is to put forth an overarching information security policy for a general physicians’ clinic. The need for information security in this type of organization is incredibly demanding and a necessity for the safety of patients, employees, and its own organizational liability.

Hypothetically located in New York, U.S., this general physicians’ clinic has roughly 100 employees, and approximately 1,500 individual patients on file. Of these 100 employees, several of them work within the Information Security (InfoSec) department, which is a separate division from the Information Technology (IT) department. This document’s purpose is to set up InfoSec policies to protect this organization from threats.

The first sections of this document, up to “Policies”, covers essentially what is the enterprise information security policy, which prepares the climate and environment of Information security for this organization.

A [?] with a number inside the brackets indicates a source was used that was numbered down below in the “References” section. Numbers were used instead of in-text citations to save complexity and space.

1. Scope

This document's scope refers to the range of topics covered in InfoSec. Because security can potentially encompass all aspects of an organization, it is exceedingly difficult to gauge what exactly will be needed in the future for a first draft. However, this document plans to cover the following, initially:

* vision, mission, goals, and objectives of this security plan,
* information assets,
* greatest threats,
* associated hardware and software,
* legal liabilities,
* roles and responsibilities of groups of employees,
* authorized and unauthorized use of technology,
* enterprise, issue, and system specific policies,
* standards, practices,
* risk management,
* incident response,
* violations of policy, and
* future review of policy.

Because “scope creep” can eventually invade this document, it is important that “future reviews of policy” carefully consider adding new elements to the scope of this document, especially if it is not related to InfoSec.

1. Information Assets

This part of the security policy document lists out some of the information assets that will be critical to track in our organization.

* 1. Patient Information

Patient data exists across several categories, such as personally identifiable information (PII), medical records, or insurance information.

**Table 1.1**

**Examples of Patient Medical Data**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Medical history | Height, weight, age | General physician contact | Dental records [1] | Surgical records [1] | Behavioral data (diet, smoking, drugs) [1] |
| Biometrics (blood pressure) [1] | Living conditions (house, family) [1] | Diseases, disorders | Diagnosis [2] | Demographics (religion, creed, nationality, origin) [2] | Exposures (asbestos, arsenic, poisons) [2] |
| Medical/laboratory test results [2] | Genetic information | Family history | Prescriptions | Allergies | Vitals |

According to the Privacy Rule provision to HIPAA, several of these patient data categories are under the description of “Protected Health Information” [4]. These include past, present, or future health information that may identify the individual. Only under abnormal circumstances can these categories of information be disclosed. The following table details some examples “personally identifiable information” that are also important to consider.

**Table 1.2**

**Examples of Patient Personally Identifiable Information**

|  |  |  |  |
| --- | --- | --- | --- |
| Full name | Address(s) | Social Security # | Telephone # |
| Email address(s) | Gender | Race | Birthday |
| Geographic indicator(s) |  |  |  |

Other forms of miscellaneous patient data that may be present in our patient records would be insurance information (provider, deductibles, coverage), or billing information.

* 1. Employee Information

**Table 1.3**

**Examples of Employee Information**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Tax information | Payroll | Scheduling | Full name | Address(s) |
| Social Security # | Telephone # | Credit background | Email address(s) | Gender |
| Race | Birthday | Criminal history | Resume, employment history |  |

Employee information contains critical personally identifiable information such as tax information and social security numbers. According to the IRS tax return information cannot be disclosed unless permitted by statue.

* 1. Organizational Information

Organizational information may include documentation (such as this one) of policies, procedures, workflows, standards, practices, or other forms of media. These documents may exist in a physical or digital format. In either case, these documents should not be viewable to specific employees depending on the importance of each document.

D. Greatest Threats

Currently the biggest threats to web applications according to the OWASP Top Ten as of drafting this document are: broken access control, cryptographic failures, injection, insecure design, security misconfiguration, vulnerable and outdated components, identification and authentication failures, software and data integrity failures, security logging and monitoring failures, and server-side request forgery (SSRF) [11].

This document should focus on the core issues that arise because of these vulnerabilities.

* 1. Likely Threat Actors

Because of the nature of risk associated with a potential breach of PHI and PII, the greatest threat actors to this organization are assumed to be individuals engaged in ransomware.

Ransomware is an event in which an attacker has stolen information and requests that the victim pays for it back or to minimize damages. It is imperative that this cost is not paid for in any capacity and that local authorities are notified. Furthermore, risk assessments must be completed to overview the potential loss and how it can be mitigated further afterwards. Review the “Breach Notification Policy” for more information.

Additionally, threat actors may include accidental security breaches internal to the organization.

1. **Hardware, Software**
   1. Database Management System & Security

Online sources claim that with the rise of electronic health records (EHRs), more third-party database software has been marketed and used in the industry. However, with third-party software this has led to the unwillingness and accidental leak of patient information. Therefore, we make the claim that a custom developed system that makes the full use of its tools is the best option for this clinic's future.

* 1. **Database Software:** Oracle Enterprise Database 12.1.

This database software has professional level security mechanisms and backup capabilities. Oracle Enterprise cooperates nicely with programming languages like Java, meaning a prominent level of security is attainable [7]. Oracle Enterprise contains a variety of data backup and security configurations that can be used to attain high security.

* 1. Development Programming Languages

**Programming Language(s):** Java

Java is one of the most secure programming languages that professional organizations use in the modern day. Java can provide “internal data management,” “automated memory management,” “error detection and handling,” “secure garbage collection,” “private keywords,” and “foolproof data type checking” [8]. These 6 features place it over older programming languages such as C or C++ that do not have these features which open possibilities of exploitation.

* 1. Firewall: Packet filtering, static firewall system

A static firewall system allows routers on our configured network to block traffic from packets determined to be potentially malicious. Static firewalls provide a way to consistently deny traffic from established untrusted protocols or addresses.

1. **Liabilities**

HIPAA Guidelines

* 1. **The Health Insurance Portability and Accountability Act (HIPAA**) is a set of federal laws that regulate the storage, processing, and transmission of healthcare information. Several provisions exist regarding HIPAA.
  2. **Privacy Rule**: “set national standards for the protection of individually identifiable health information by [healthcare] entities”, healthcare entities including this one [9].
  3. **Security Rule**: “sets national standards for protecting the confidentiality, integrity, and availability of electronic protected health information” [8].
  4. **Enforcement Rule**: “provides standards for the enforcement of all the Administrative Simplification Rules” [8].
  5. **Omnibus Rule**: “implements a number of provisions of the HITECH Act to strengthen the privacy and security protections for health information established under HIPAA” [8].
  6. **Breach Notification Rule**: This organization will be required to notify "the individual, the media, and the Secretary [of the U.S. Dept. of HHS]”. A data breach is classified as “impermissible use and disclosure of personally identifiable health information” if the probability that the said information has been compromised based on a “risk assessment of the following factors”:
* “The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
* the unauthorized persons whom used the protected health information or to whom the disclosure was made to;
* whether the information was actually viewed or acquired; and
* the extent to which the risk to the protected health information has been mitigated.” [12].

HIPAA also requires as part of the Security Rule and Privacy Rule that most PHI must be encrypted. In the case that unauthorized access to PHI has been determined to have occurred, this data must be purged using either physical or digital methods. Physical media can be shredded or destroyed (CDs, paper documents, or film). Digital media can be destroyed or purged in a manner consistent with NIST Special Publication 800-88, “Guidelines for Media Sanitation” [13].

These basic ideas will cover the basis of several policies, standards, procedures, and guidelines found in this document.

* 1. Federal Privacy Act
* “Protects records about individuals retrieved by personal identifiers (PII)” [10].
* “An individual has rights under the Privacy Act to seek access to and request correction” to personal records [10].
* “Prohibits disclosure of such records without the prior, written consent of the individual(s) to whom the records pertain” [10].
  + This federal Act is the basis for regulating and maintaining the policies and security of PII in the organization.

1. **Roles and Responsibilities**

Through this security policy document, different roles and their responsibilities of information security officers/ analysts will be covered in regards to a physician’s clinic.

Chief Information Officer (CIO): The CIO would be responsible for overseeing the organization's overall information security strategy and managing the Information Security department. They would ensure that the Information Security policies and procedures are up to date and enforced, along with monitoring these policies. They would also be an integral part of the senior management team on the clinic’s board of directors and would maintain the clinic’s security posture.

Security Analysts: Security Analysts would be responsible for monitoring the clinic's network and systems for security breaches, vulnerabilities, and risks. They would conduct regular security assessments and vulnerability testing to identify potential security threats. They would also be responsible for implementing security measures to protect the clinic's information assets and data. In case of any security incidents, they would investigate with the incident response team and resolve them.

Incident Response Team: This team would be responsible for responding to and managing security incidents, such as malware incidents, network intrusions, data breaches, and other security-related incidents. They would work closely with the security analysts to identify and resolve any security incidents and implement necessary security measures.

System Administrator: This role would be responsible for managing the clinic's information systems, including servers, databases, applications, and network devices. They would implement security measures to protect the clinic's information assets and data. They would also ensure that system software and hardware are up to date with the latest security patches and updates.

General Employees: All employees would be responsible for maintaining the confidentiality, integrity, and availability (CIA triad) of the clinic's information assets and data. They would be required to comply with all of the information security policies and procedures, including password policies (covered ahead), data classification, and access controls. They would also be responsible for reporting any security incidents or breaches to the Incident Response Team immediately. This is where the annual security awareness training comes into place – ensuring that any updates or new policies have been promoted.

1. **Policies**
   1. Issue Policies

Proper Computer Use Policy

Employees are authorized to use company provided computers or other technology to help persist their job workflows. Accessing unknown or forbidden websites on company provided equipment can pose security risks to the organization. Other equipment such as printers, fax machines, or phones provided by the organization should and will only be used for organizational purposes.

Email Policy

Employees logged into the organization’s network are required to use the email provided to them upon hire. Emails originating not from the organization’s domain will have tags on them in apparent text that will signal the reader to proceed with caution as the email originated from outside the organization.

Communication with organizations or individuals from outside the organization should be kept to a minimum and only through customer service experience. All users who receive phishing, scamming, or malicious emails must notify the InfoSec staff of the sender, the content, and nature of the threat as soon as possible.

Communication of personal healthcare information over email unless to the individual or cleared through HIPAA’s Disclosure Rules is also prohibited. The identity of the person whom to be sent to must have an email which can be verified to the correct individual.

Individual Identification Policy

To identify an individual electronically, employees must verify individual identity using information already stored on site. Personally identifiable information (PII) such as address(s), home, full name, social security number, or email address(s) can be used to verify the identity of an individual.

Incidents of false positive individual identifications should be treated as a breach and should then be reported to InfoSec staff.

External Storage Device Policy

External storage devices include but are not limited to: USBs, portable hard drives/SSDs, micro SDs, portable computers, CDs, DVDs, or film.

Personal use of these to backup healthcare information is prohibited. On premises, only the dedicated services used to store and backup this information can be used to store this information.

Internet Use Policy

Internet use on site is only prohibited on devices that do not have root access to critical data systems. Otherwise, Internet usage is permitted on safe, protected networks on-site.

Printing Policy

Physical documents can be printed, but if they contain PHI, they are required to be locked and inaccessible to non-employees, unless for HIPAA’s disclosure reasons.

Anti-Malware Policy

To protect employees from accessing the Internet, anti-malware will be required to be installed on all company computers and cannot be removed or disabled from the device for any reason. Only in permitted circumstances can anti-malware be removed in the following case: InfoSec group unanimously agrees no risk would be taken for free upon removal. The software is currently impeding workflow and must be disabled.

Phone Policy

Use of personal phones will not be permitted on premises (unless for emergencies and break room) and cannot be connected to the organization network.

Authorized Access Policy

Only employees involved in healthcare are permitted to view healthcare information pertaining to patients. Only written permission can be gained by the individual to disclose PHI. See the policy below for more details.

PHI Disclosure Policy

PHI according to HIPAA’s Privacy Rule and their Disclosure Rules only allows disclosure of personal healthcare information under the following reasons:

1. To the individual;
2. Treatment, payment, or healthcare operations;
3. Uses and disclosures with opportunity to agree or object by the individual (in cases of incapacitation, it is up to the entity to make the judgement based on the best interests of the individual);
4. Incidental use and disclosure (all information that was accidentally shared must be as minimal as possible);
5. Public interest and benefit activities (required by law, public health activities, victims of abuse, health oversight activities, judicial and administrative proceedings, law enforcement purposes, decedents, organ donation, research, serious threat to health or safety, essential government functions, or workers compensation laws);
6. Limited data set (personally identifiable information has been removed) [3].

Breach Notification Policy

A breach of healthcare data is defined as:

* The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
* The unauthorized person who used the protected health information or to whom the disclosure was made;
* Whether the protected health information was actually acquired or viewed; an
* The extent to which the risk to the protected health information has been mitigated.

Upon a breach of data, this organization will be required to notify:

* The individual;
* The media; and
* Secretary of the U.S. Department of Health and Human Services [12].

For this organization, it will be required for all employees after a data breach to attend a scheduled SETA training to help remind all employees of the risks and liabilities associated with a breach.

After a breach, the InfoSec group will be required to investigate to collect as much information as possible for not only the federal government and media, but also to ensure that the nature of the breach does not happen again.

HIPAA Consistent Compliance Policy

HIPAA’s Privacy Rule requires entities to ensure compliance with HIPAA to the federal government.

* Requirement to provide records and proof of compliance reports;
* Cooperate with complaint investigations and compliance reviews (by the Secretary).

Compliance reports are defined as proof of proper security measures taken to reduce the risk of data breach of personally identifiable health information.

Data Sanitization Policy

HIPAA’s Security Rule calls for data sanitization in the incident of data loss through attacks. It recommends following NIST Special Publication 800-88 to sanitize digital data.

* Cryptographic erase (CE) methods
* Self-Encrypting Drives (SEDs) [17].

NIST 800-88 also recommends to “categorize the information, assess the nature of the medium on which it is recorded, assess the risk to confidentiality, and determine the future plans for the media” [17].

CE methods should not be used in the following situations:

* “If encryption was enabled after sensitive data was stored on the device without having been sanitized first”;
* “Whether sensitive data was stored on the device without being sanitized prior to encryption” [17].

* 1. System Policies

Network Policy

This policy defines guidelines and best practices for network usage within the clinic's premises. This covers wireless network policies, monitoring and compliance tools that specify monitoring procedures and consequences for non-compliance with network policies.

The private network should only be accessible to employees with OS level accounts with the securities in place for those accounts. This private network should require that Ethernet connections are used instead of wireless ones, to prevent packet sniffing at any capacity over wireless connections.

The private network has a VPN service to the public network which has access to the Internet through a firewall. This allows only safe traffic to enter the organization as traffic can be easily identified through one location and creates a DMZ zone for which protects data in the organization.

VPN Policy

This policy defines guidelines for using virtual private networks (VPNs) to securely access the clinic's network remotely. This allows necessary security measures, such as encryption and authentication protocols, for VPN connections.

For some workflows, it may be required that VPNs are used by employees. VPNs are required to use encryption throughout the entire process in which it transmits data.

Firewall Policy

This policy defines guidelines for the configuration and management of the clinic's firewall system to protect the network from unauthorized access and external threats. It also specified the rules and restrictions for inbound and outbound traffic.

A packet-filtering, static filtering firewall is most appropriate for this organization as it can adapt willingly, as dynamic filtering poses problems that may be easily resolved by thorough analysis of logs and network traffic. VPNs are required to enter through this firewall to maintain deperimeterization.

Database Security Policy

This policy defines guidelines for securing patient and clinic data stored in databases. It defines roles and permissions for accessing and modifying data based on job responsibilities and the principle of least privilege.

Database security is best managed through proper configuration of the security features in place. In our example, Oracle Enterprise, it comes along with several security features like data encryption, user groups, and user permissions to help maintain security through proper configuration. Proper configuration is incredibly important as this issue is consistently present in the OWASP Top Ten.

Physical Security Policy

Physical security refers to security maintain physical, typically paper documents. Although most PII or PHI should be made electronic as much as possible, security for physical documents is required. For storage, these documents must be behind some lock mechanism where they will be required to be opened by key.

In processing, these physical documents should be hidden from plain sight behind paned glass, and only be shared with the individual or for other reasons disclosed in HIPAA’s Disclosure Rules.

Physical information, if needing disposal, should be destroyed through chemical means. A locked recycling bin that allows entry of paper and other physical documents will be taken by an external organization to be decomposed through chemical means, by far the safest means of physical document elimination.

Two Factor Authentication Policy

To log into on-site accounts, employees must use a two-factor authentication system with either a mobile SMS text message or a robot call. They can ask that a device be saved for that account for up to 14 days, after which it will be required to conduct two-factor authentication again.

Access Control List Policy

This policy defines guidelines for managing access control lists (ACLs) that determine network access permissions. It specifies rules for granting or denying access based on user roles, IP addresses, and other relevant criteria.

User roles should follow the principle of “least privilege” as they are configured into access control lists.

Encryption Policy

This policy defines guidelines for encryption mechanisms to protect sensitive data within the clinic's network and systems. It also includes encryption algorithms and protocols to be used for data in transit and data at rest, along with procedures for secure generation, storage, and distribution of encryption keys.

All PHI and PII must be encrypted in storage, in processing, and in transmission on logical storage devices to maintain compliance with HIPAA’s Security Rule.

In storage encryption can be accomplished with proper database configuration to enable schema encryption. It can also be accomplished with OS level encryption, ensuring proper security at a lower stack level.

In processing and in transmission encryption can be accomplished using Web protocols such as HTTPS (Hypertext Transfer Protocol Secure), IPsec, TCP, and SSH (Secure Shell). TCP helps verify the data integrity of a connection using handshake algorithms to maintain connection between computers.

1. Standards

This section of the security policy document will provide a set of guidelines and best practices for employees to follow when handling sensitive information and tasks related to information security. Integrating and enforcing these standards within the security policy document fosters a culture of security awareness and responsible information security throughout the clinic.

Policy Behavior

Policy Behavior refers to the conduct and adherence to information security policies within the physician’s clinic. Regarding the established policies above, it revolves around understanding the purpose of each policy, following the specified procedures, and being aware of the potential consequences of any violations.

Secure Coding

This standard revolves around industry best practices and coding guidelines to minimize vulnerabilities and protect against potential threats. For example, coding practices like using encapsulation, private keywords, automatic memory management, prepared statements, filtering and flagging and encryption in transmission are all examples secure coding practices [14].

1. Practices

A physician’s clinic must have a comprehensive security policy that addresses various practices to ensure the confidentiality, integrity, and availability (CIA triad) of sensitive information and data. Two important practices that this security policy document will cover are password policies and information sharing (patients) in public.

Password Policy

Employees are expected to have personal accounts on site to access their work items and other miscellaneous work. Passwords will be required to be created by each employee for their accounts, for which they can access on any machine if they so wish to.

Passwords must fill in the following categories:

* Be at least 15 characters long.
* Password must be changed every 60 days (alongside HIPAA’s Breach Notification Rule)
* Not be similar to the last 2 passwords
* Contain at least 3 symbols and 3 numbers
* Does not exist in already established rainbow tables online

This password policy is expected to outlast any brute force attempt by any modern computer. Passwords are expected to be stored in a hashed format in SHA-256, an incredibly secure encryption algorithm. This policy is expected to change in the future once cryptographic algorithms begin to be solved by widespread quantum computing.

Sharing Patient Information (in public)

Sharing patient information in public can lead to serious breaches of patient confidentiality, which can result in legal and financial consequences for the clinic. According to the HIPAA Privacy Rule, healthcare providers must implement safeguards to protect the privacy of patient information.

Employees should be aware of the sensitivity of patient information and avoid discussing it in public areas, such as elevators or waiting rooms. Attacks known as “shoulder peeking/shoulder surfing” or simply listening in public can be a potential breach of security and could potentially require notification to authorities if the risk identified was severe enough. Employees should be trained to identify and report any potential breaches of patient confidentiality, such as unauthorized access to medical records or data theft.

1. Programs

Risk Management

Risk management is a critical component of maintaining a secure environment within a physician's clinic. One key aspect of risk management is conducting periodic evaluations to ensure the effectiveness of implemented security measures and to identify any emerging risks. The clinic will be required to conduct risk assessments to comply with HIPAA’s Privacy Rule. As part of compliance, risk assessments give the ability to measure the actual risk of certain healthcare data being accidentally disclosed. A reasonable risk assessment could prevent otherwise dangerous costs to the clinic if the risk associated with a breach is too high to neglect.

A risk assessment should ask the following questions:

* Risk identification (what data is potentially under attack?)
* Risk analysis (how dangerous is a potential breach?)
* Risk evaluation (what is our current risk appetite?)
* Risk treatment (how do we bring our current risk lower?)

Answering this question will mold a risk assessment which then can be used to document and research more about what can be done about a category of data.

Periodic Evaluations

Regular evaluations should be performed to assess the clinic's security posture. These evaluations can be security audits, vulnerability assessments, penetration testing, and other relevant security assessments. By conducting these assessments on a recurring basis, the clinic can identify vulnerabilities, weaknesses, or gaps in its security components. Based on the physician’s clinic size, periodic evaluations can occur annually.

Security audits, and potentially vulnerability assessments, should ask the following questions:

* How well are we protecting data in storage, in transmission, and in processing?
* How well has the organization kept the confidentiality, integrity, and availability of our data?
* How well have employees followed and learned from policies, practices, standards, programs, and procedures?
* What is our current risk appetite? What data is at risk? How can we further mitigate any existing risks?
* Penetration testing also assists in periodic evaluations. They will be expected to be outsourced from trusted outside organizations.
* Use penetration testing to test specific aspects of our information systems.
* What errors are we making in our code?
* Are there any aspects of secure coding principles we are neglecting to follow?

The results of security audits, vulnerability assessments, and penetration tests can then be used to make changes to existing policy and address issues that were identified during the periodic review process.

Cost Benefit Analysis

It is important to conduct a cost-benefit analysis regarding security investments, especially in a health clinic. This analysis involves assessing the costs associated with implementing security measures against the potential benefits they offer. Some factors to consider include:

* Likelihood of threats
* Potential impact of security incidents
* Costs of implementing security controls
* Potential cost savings from preventing or mitigating security breaches.

By conducting a comprehensive cost benefit analysis, the clinic can prioritize security investments and allocate resources effectively, ensuring an optimal balance between security and cost. From a security standpoint, it is essential for the clinic to establish a systematic and well-documented approach for periodic evaluations and cost benefit analyses, tailored to its specific circumstances and requirements.

SETA Program

Employees within the organization must be trained and be familiar with security threats to reduce incidents as much as possible. Overview of policies, procedures, and practices must be in place to remind employees of the potential threat of breaches. The idea of using a SETA program is to accomplish the following: “Improve awareness of system resources, developing skills and knowledge to use technology more securely,” and “building in-depth knowledge to design security programs” [18].

Therefore, the following SETA program should be scheduled if required by the organization:

1. Awareness
2. Current and trending threats to cyber-security at the time.
3. Recent breaches in the healthcare industry.
4. Statistics related to phishing, ransomware, and scams online.
5. Training
6. Highlight phishing examples.
7. Breakout groups to determine whether an email was a malicious attempt.
8. What to do if someone asks to see healthcare information.
9. Education
10. Remind employees why security in healthcare is so important.
11. Potential impact on friends, family, the organization, and yourself on the occurrence of a breach.
12. What you should do to teach others about cybersecurity in healthcare.

This SETA program framework is tentative to change depending on the changing climate of the organization’s liabilities, size, and current threats to cybersecurity.

1. Incident Response

In an incident response plan, it is crucial to establish clear roles and responsibilities for the Incident Response team. This way the team is prepared and can respond effectively to several types of security incidents.

Disaster Recovery Plan: A disaster recovery plan should include a thorough assessment of potential risks and vulnerabilities, such as natural disasters, system errors and issues, or cyber threats. It is important to regularly test and validate the plan through simulated scenarios to identify any gaps or weaknesses. Other options like off-site backups, duplicate systems, and alternative infrastructure systems should be considered to ensure the continuity of critical operations.

Incident Response Plan: An incident response plan should include procedures and checklists to guide the response team in handling specific types of incidents. This can include steps for initial assessment, evidence preservation, forensic analysis, and communication with relevant stakeholders. The plan should also address legal requirements, such as incident reporting obligations, essential for all organizations.

One example of an incident response plan that future IRPs can follow can closely resemble a Check List Guide from the U.S. Department of Health and Human Services:

* “Execute a response and mitigation procedures and contingency plans;
* Report the crime to other law enforcement agencies, including but not limited to the FBI, Secret Service, or local law enforcement.
* Report all cyber threat indicators to federal and information-sharing and analysis organizations (ISAOs), including but not limited to the Department of Homeland Security, the HHS Assistant Secretary for Preparedness and Response, and private sector cyber-threat ISAOs.
* Report the breach to the Office for Civil Rights under the U.S. Department of Health and Human Services as soon as possible, but no later than 60 days after the discovery of the breach affecting more than 500 individuals” [15].

Business Continuity Plan: A business continuity plan should identify vital business functions, dependencies, and recovery strategies to ensure the clinic can continue operating during and after a disruptive incident. As a health clinic in society, communication plans need to be established for informing about any impacts on the normal routine to relevant individuals and groups.

Power Outages: To navigate through the impact of power outages, the clinic can implement uninterrupted power supply (UPS) systems or backup generators to ensure continuous power to critical infrastructure and equipment. As a health clinic, it is important to conduct regular maintenance and testing of backup power systems to ensure their reliability. Communication plans should be in place to inform staff, patients, and relevant officers about power outage situations and the next steps.

Data Backup: A data backup strategy involves regular backups of vital data, ensuring redundancy and availability in the event of data loss or corruption.  It is important to prioritize the backup of patient health records, medical databases, and other sensitive information. Regular testing and restoration of backups should be conducted to verify their integrity and effectiveness.

1. Future Review

Periodic Review of Overall Policy

Part of the Periodic Evaluation of this clinic’s security is to take part in OWASP’s Top Ten threats at any time. As previously mentioned, OWASP’s Top Ten threats show the biggest threats to developers and web application security. The organization must keep these top threats in mind during the Periodic Evaluations to improve the clinic’s security. It is also important to model and review from international cybersecurity forums and organizations new cybersecurity measures to protect information systems from attack. Some organizations include the International Information System Security Certification Consortium (ISC)2, the Cybersecurity and Infrastructure Security Agency (CISA). With these in mind, periodic evaluations, and periodic review of overall policy can help provide this organization with the best possible policy it can use to maintain security at a high level.

1. References

[1] *Big data in health care and patient outcomes*. School of Public Health. (2022, September 15). <https://publichealth.tulane.edu/blog/big-data-in-healthcare/>

[2] “Clinical Data - GDC Docs.” Docs.gdc.cancer.gov, docs.gdc.cancer.gov/Encyclopedia/pages/Clinical\_Data/. ‌

‌[3] United States Department of Health and Human Services. SUMMARY of the HIPAA PRIVACY RULE. May 2003.

‌[4] U.S. Department of Labor. “Guidance on the Protection of Personal Identifiable Information | U.S. Department of Labor.” Dol.gov, 2019, www.dol.gov/general/ppii.

[5] N Basil, Nduma. Protecting Federal Tax Information For. Cureus, Oct. 2022.

[6] Oracle. “Oracle Enterprise Database Service.” Oracle.com, 2023, [www.oracle.com/database/enterprise/](http://www.oracle.com/database/enterprise/).

[7] @technologynews. “Types of Medical Databases and Their Benefits for Humanity | Hacker Noon.” Hackernoon.com, May 2021, hackernoon.com/types-of-medical-databases-and-their-benefits-for-humanity-gk1j34a3.

[8] Bicknell, Andin. “6 Reasons Why Java Is More Secure than Other Languages.” Educative: Interactive Courses for Software Developers, educative, 10 Jan. 2019, [www.educative.io/blog/why-java-is-more-secure-than-other-languages](http://www.educative.io/blog/why-java-is-more-secure-than-other-languages).

[9] U.S. Department of Health & Human Services. “HIPAA for Professionals.” HHS.gov, 2021, www.hhs.gov/hipaa/for-professionals/index.html. Accessed 17 May 2021.

[10] Freedom of Information Act (FOIA) Division, Assistant Secretary for Public Affairs (ASPA. “The Privacy Act.” HHS.gov, 11 July 2019, www.hhs.gov/foia/privacy/index.html.

‌[11] OWASP. “OWASP Top Ten.” Owasp.org, OWASP, 2021, owasp.org/www-project-top-ten/.

[12] Office for Civil Rights. “Breach Notification Rule.” HHS.gov, 14 Sept. 2009, www.hhs.gov/hipaa/for-professionals/breach-notification/index.html.

‌[13] Kissel, Richard, et al. “Guidelines for Media Sanitization.” Csrc.nist.gov, 17 Dec. 2014, csrc.nist.gov/publications/detail/sp/800-88/rev-1/final.

[14] OWASP. “OWASP Secure Coding Practices-Quick Reference Guide.” Owasp.org, owasp.org/www-project-secure-coding-practices-quick-reference-guide/.

[15] U.S. Department of HHS. My Entity Just Experienced a Cyber-Attack! What Do We Do Now? May 2021.

[16] Drabant, Anna, and HHS Office of Civil Rights. HIPAA Administrative Simplification Regulation Text. 2013.

‌ [17] ---. “Guidelines for Media Sanitization.” NIST, vol. 800, no. 88, Dec. 2014, nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf, <https://doi.org/10.6028/nist.sp.800-88r1>.

[18] Whitman, Michael, E. and Herbert J. Mattord. Principles of Information Security. Available from: VitalSource Bookshelf, (7th Edition).

.