THE PHYSICIAN'S HIPAA REFERENCE GUIDE

Please Note:

Any organization that stores, processes or transmits personal health information (PHI) is required to comply with the Health Insurance Portability and Accountability Act (HIPAA) and safeguard all protected data. The related HITECH Act mandates securing a new regime of electronic health records (EHR) — and prescribes stiff penalties for organizations that fail to do so. Compliance entails deployment of security controls and processes to fulfill the laws.

INTRODUCTION:

It is amazing how much responsibility Small-Practice Physicians have to handle. They typically see many patients daily, trying to tend to their needs. Then there are personnel issues, insurance issues, equipment issues, technology issues, and to top it all off, compliance issues as well. That puts a lot of pressure and strain on their shoulders.

When it comes to worrying about HIPAA compliance many Physicians put forth their best effort to be compliant. They are well aware of the risks and liability that non-compliance poses. Most Physicians typically have a good grasp of the HIPAA Privacy rule, being very diligent at addressing privacy requirements, but when it comes to security they are often at a loss. The HIPAA Security Rule has a lot of technical requirements and it involves many network and computer security details which someone without a technical background might not fully understand.

Our intent with this guide is to raise awareness of the HIPAA Security Rule requirements, and what steps can be taken to ensure compliance. We hope this helps Physicians understand the issues and details around protecting and securing electronic patient information. Unless the Physician has a technical background, network security can easily be overwhelming, with many crucial areas being missed. However, HIPAA compliance with the Security Rule can be attainable.

The Physician's HIPAA Reference Guide is specifically designed for Small-Practice Physicians. It covers the relevant aspects of HIPAA for Physicians, but has been streamlined for ease of use. Topics include the legal background on HIPAA, PHI, Business Associates, and the Privacy Rule. We have also included a detailed overview of the Security Rule, Breach Notification, and Compliance Enforcement as well as Measurable Steps you can take to ensure compliance. This Reference Guide is available in PDF format, but is designed to be used as a desk reference, as each section is tabbed for quick reference. We hope you find it useful and informative.

TABLE OF CONTENTS

i

LEGAL BACKGROUND

ABOUT HIPAA / HITECH

HIPAA is U.S. Public Law 104-191 — the Health Insurance Portability and Accountability Act of 1996. Congress created the Act to improve health care enabled by the nation's health plans and providers. HIPAA mandates standards-based implementations of security controls by all health care organizations that create, store or transmit electronic protected health information (PHI). The HIPAA Security Rule governs protection of PHI. Organizations must certify their security programs via self-certification or by a private accreditation entity. Non-compliance can trigger various civil penalties, including fines and/or imprisonment.

HITECH is the Health Information Technology for Economic and Clinical Health Act, which brings additional compliance standards to healthcare organizations. It is directly related to HIPAA, and was part of the American Recovery and Reinvestment Act of 2009. HITECH requires healthcare organizations to apply "meaningful use" of security technology to ensure the confidentiality, integrity, and availability of protected data. Detailed requirements for HIPAA and HITECH are managed by Department of Health and Human Services (HHS).

On Jan. 25, 2013, the Department of Health and Human Services (HHS) published the “HIPAA Omnibus Rule,” a set of final regulations modifying the Health Insurance Portability and Accountability Act (HIPAA) Privacy, Security, and Enforcement Rules to implement various provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act.

Security is a crucial part of HIPAA / HITECH. The Department of Health and Human Services states, "[It] is important to recognize that security is not a one-time project, but rather an ongoing, dynamic process." HIPAA therefore requires security-related processes. HIPAA regulations do not mandate particular security technologies. Instead, they specify a set of principles for guiding technology choices.

PROTECTED HEALTH INFORMATION (PHI)

PHI falls under the Privacy Rule. However, as e-PHI is simply PHI in electronic form, it is pertinent to include this section to review exactly what HHS considers PHI. According to the US Department of Health and Human Services, protected health information (PHI) is individually identifiable information that is:

1. *Except as provided in item 2 of this definition,*
   - i. *Transmitted by electronic media;*
   - ii. *Maintained in electronic media; or*
   - iii. *Transmitted or maintained in any other form or medium (includes paper and oral communication).*
2. *Protected health information excludes individually identifiable health information:*
   - i. *In education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;*
   - ii. *In records described at 20 U.S.C. 1232g(a)(4)(B)(iv);*
   - iii. *In employment records held by a covered entity (see below for definition) In its role as employer; and*
   - iv. *Regarding a person who has been deceased for more than 50 years.*

Individually identifiable health information is information that is a subset of health information, including demographic information collected from an individual, and

1. *Is created, or received by a health care provider, health plan, or health care clearing house; and*
2. *Relates to past, present, or future physical or mental health conditions of an individual; the provision of health care to the individual; or past, present, or future payment for health care to an individual, and*
   - i. *That identifies the individual; or*
   - ii. *With respect to which there is a reasonable basis to believe the information can be used to identify the individual.*

Individually identifiable health information (i.e., PHI) is subject to state and federal privacy and security rules including, but not limited to, the Health Insurance Portability and Accountability Act (HIPAA).

A covered entity is any health plan, health care clearing house, or health care provider who transmits any health information in electronic form in connection with a qualified transaction as well as any business associates.

Data are "individually identifiable" if they include any of the 18 types of identifiers for an individual or for the individual's employer or family member, or if the provider or researcher is aware that the information could be used, either alone or in combination with other information, to identify an individual.

These identifiers are:

- Name
- Address (all geographic subdivisions smaller than state, including street address, city, county, or ZIP code)
- All elements (except years) of dates related to an individual (including birth date, admission date, discharge date, date of death, and exact age if over 89)
- Telephone numbers
- FAX number
- Email address
- Social Security number
- Medical record number
- Health plan beneficiary number
- Account number
- Certificate/license number
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers or serial numbers
- Web URLs
- IP address
- Biometric identifiers, including finger or voice prints
- Full-face photographic images and any comparable images
- Any other unique identifying number, characteristic, or code

All protected health information is subject to federal Health Insurance Portability and Accountability Act (HIPAA) regulation.

BUSINESS ASSOCIATES

All too often, practices fail to obtain proper assurances from business associates that they are implementing proper safeguards to protect PHI & e-PHI. Recently, HHS has come down very hard on covered entities and business associates for failing to comply with HIPAA regulations.

A “business associate” is any person or entity that performs certain functions that involve the use or disclosure of PHI on behalf of, or provides services to, a covered entity. A covered entity (health provider, clearing house, etc) can function as a business associate of another covered entity. Some activities that constitute a business associate include health care operations, third party billing, CPAs, a health care clearinghouse, lawyers, or even an outsourced IT service provider.

According to 45 CFR 160.103: *The Privacy Rule requires that a covered entity obtain satisfactory assurances from its business associate that the business associate will appropriately safeguard the protected health information it receives or creates on behalf of the covered entity. The satisfactory assurances must be in writing, whether in the form of a contract or other agreement between the covered entity and the business associate.*

A covered entity’s contract or other written arrangement with its business associate must contain the elements specified at 45 CFR 164.504(e). For example, the contract must:

- *Describe the permitted and required uses of protected health information by the business associate*
- *Provide that the business associate will not use or further disclose the protected health information other than as permitted or required by the contract or as required by law*
- *Require the business associate to use appropriate safeguards to prevent a use or disclosure of the protected health information other than as provided for by the contract.*

Where a covered entity knows of a material breach or violation by the business associate of the contract or agreement, the covered entity is required to take reasonable steps to cure the breach or end the violation, and if such steps are unsuccessful, to terminate the contract or arrangement. If termination of the contract or agreement is not feasible, a covered entity is required to report the problem to the Department of Health and Human Services (HHS) Office for Civil Rights (OCR).

HIPAA PRIVACY RULE

The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically.

The Privacy Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Privacy Rule also gives patient's rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.

USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION

According to the US Department of Health and Human Services, the general rules governing use and disclosure of PHI are as follows:

(1) Covered entities: Permitted uses and disclosures. A covered entity is permitted to use or disclose protected health information as follows:

(i) To the individual;

(ii) For treatment, payment, or healthcare operations, as permitted by and in compliance with § 164.506;

(iii) Incident to a use or disclosure otherwise permitted or required by this subpart, provided that the covered entity has complied with the applicable requirements of §§ 164.502(b), 164.514(d), and 164.530(c) with respect to such otherwise permitted or required use or disclosure;

(iv) Except for uses and disclosures prohibited under § 164.502(a)(5)(i)pursuant to and in compliance with valid authorization under § 164.508

(v) Pursuant to an agreement under, or as otherwise permitted by, § 164.510;

(vi) As permitted by and in compliance with this section, § 164.512, § 164.514(e), (f), or (g).

(2) Covered entities: Required disclosures. A covered entity is required to disclose protected health information:

(i) To an individual, when requested under, and required by § 164.524 or§ 164.528; and

(ii) When required by the Secretary under subpart C of part 160 of this subchapter to investigate or determine the covered entity's compliance with this subchapter.

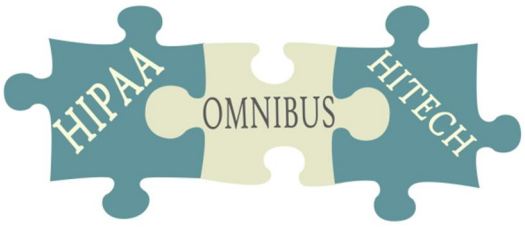
(3) Business associates: Permitted uses and disclosures. A business associate may use or disclose protected health information only as permitted or required by its business associate contract or other arrangement pursuant to § 164.504(or as required by law. The business associate may not use or disclose protected health information in a manner that would violate the requirements of this subpart, if done by the covered entity, except for the purposes specified under § 164.504(e)(2)(i)(A) or (B) if such uses or disclosures are permitted by its contract or other arrangement.

(4) Business associates: Required uses and disclosures. A business associate is required to disclose protected health information:

(i) When required by the Secretary under subpart C of part 160 of this subchapter to investigate or determine the business associate's compliance with this subchapter.

(ii) To the covered entity, individual, or individual's designee, as necessary to satisfy a covered entity's obligations under § 164.524(c)(2)(ii) and (3)(ii) with respect to an individual's request for an electronic copy of protected health information.

HIPAA SECURITY RULE



The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information (e-PHI) that is created, received, used, or maintained by any organization that stores, transmits, or processes personal health information (PHI). The Security Rule requires covered entities to have:

- *Documented administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of e-PHI they create, receive, maintain or transmit.*
- *Identify and protect against reasonably anticipated threats to the security or integrity of the information*
- *Protect against reasonably anticipated, impermissible uses or disclosures*
- *Ensure compliance by their workforce.*

EPHI

Electronic protected health information (ePHI) is any protected health information (PHI) that is created, stored, transmitted, or received electronically. Electronic protected health information includes any medium used to store, transmit, or receive PHI electronically.

The following and any future technologies used for accessing, transmitting, or receiving PHI electronically are covered by the HIPAA Security Rule:

- Media containing data at rest (storage)
  - Personal computers with internal hard drives used at work, home, or traveling
  - External portable hard drives, including iPods and similar devices
  - Magnetic tape
  - Removable storage devices, such as USB memory sticks, CDs, DVDs, and floppy disks
  - PDAs and smartphones

- Data in transit, via wireless, Ethernet, modem, DSL, or cable network connections
    - Email
    - File transfer

RISK ANALYSIS

A detailed risk analysis is required under the HIPAA Security Rule. It is also considered the foundation of the HIPAA Security Rule.

The Security Management Process standard in the Security Rule requires organizations to "[i]mplement policies and procedures to prevent, detect, contain, and correct security violations." (45 C.F.R. § 164.308(a)(1).) Risk analysis is one of four required implementation specifications that provide instructions to implement the Security Management Process standard. Section 164.308(a)(1)(ii)(A) states:

RISK ANALYSIS (Required).
Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (ePHI) held by the [organization].

A detailed Risk Analysis must follow the methodology described in NIST Special Publication (SP) 800-30 Revision 1. Specifically the Risk Analysis must do the following:

Risk Assessment Process

- Identify and document all ePHI repositories
- Identify and document potential threats and vulnerabilities to each repository
- Assess current security measures
- Determine the likeliness of threat occurrence
- Determine the potential impact of threat occurrence
- Determine the level of risk
- Determine additional security measures needed to lower level of risk
- Document the findings of the Risk Assessment

The Risk Assessment is a detailed report that looks at each system that contains ePHI and documents the threats to the system, the vulnerabilities to the system, the current

safeguards in place to protect the system and the additional recommended safeguards to lower the risk to the system.

ADMINISTRATIVE SAFEGUARDS

These provisions are defined in the Security Rule as the "administrative actions, policies, and procedures to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information."

These Include:

- Security Management Process
  - Covered entities must identify and analyze potential risks to e-PHI, and it must implement security measures that mitigate & minimize risks and vulnerabilities.
- Assigned Security Responsibility
  - Covered entities must designate a security official who will be responsible for developing and implementing its security policies and procedures
- Information Access Management
  - Covered entities are required to implement policies and procedures for authorizing personnel access to e-PHI only when such access is deemed necessary and appropriate.
- Security Awareness and Training
  - Covered entities must provide for appropriate authorization and supervision of staff members who work with e-PHI. All staff members must be trained on its security policies and procedures.
- Security Incident Procedure
  - Covered entities must have procedures in place and apply appropriate measures against staff members who violate them.
- Evaluation
  - Covered entities must perform periodic assessments to measure whether or not its security policies and procedures meet the requirements of the Security Rule.

PHYSICAL SAFEGUARDS

These provisions are defined as the “physical measures, policies, and procedures to protect a covered entity’s electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.”

These Include:

- Facility Access and Control
  - Covered entities must ensure that physical access to their facility is only allowed by authorized personnel.
- Workstation and Device Security
  - Covered entities must implement policies and procedures that specify the proper use and access to both workstations and electronic media. Policies and procedures must also be in place relating to the transfer, removal, disposal, and re-use of electronic media; ensuring proper protection of e-PHI.

TECHNICAL SAFEGUARDS

These provisions are defined as the “technology and the policy and procedures that protect electronic protected health information and control access to it (e-PHI).”

These Include:

- Access Control
  - Covered entities must implement technical policies and procedures that allow only authorized personnel to access e-PHI.
- Audit Control
  - Covered entities must implement technical, and/or procedural mechanisms that record and examine access and other activity in information systems that contain or use e-PHI.
- Integrity Control
  - Covered entities must implement electronic measures, as well as policies and procedures to ensure that e-PHI is not improperly altered or destroyed.
- Transmission Security
  - Covered entities must implement technical security measures to guard against unauthorized access to e-PHI transmitted over a network.

MEANINGFUL USE

Although not part of HIPAA, many providers participate in the Meaningful Use program. If your practice accepts Medicare or Medicaid, Meaningful Use will apply. CMS has indicated that Meaningful Use will be replaced with a new plan, but until it is, providers are still expected to meet the requirements if they wish to continue receiving incentive payments.

Meaningful Use requires that your EHR or EHR components must meet ONC's standards and implementation specifications, at a minimum, to be certified to support the achievement of Meaningful Use Stage 1 by eligible health care providers under the EHR Incentive Program regulations. Along with many other criteria, ONC requires that an EHR meet nine security criteria to be certified. An up-to-date list of certified EHR systems and components is posted on ONC's website.

To receive the incentive payments, you must also demonstrate that you have met the criteria for the EHR Incentive Program's privacy and security objective. This objective, "ensure adequate privacy and security protections for personal health information," is the fifth and final health policy priority of the EHR Incentive Program. The measure for Stage 1 aligns with HIPAA's administrative safeguard to conduct a security risk assessment and correct any identified deficiencies. In fact, the EHR Incentive Program's only privacy and security measure for Stage 1 is to:

> *Conduct or review a security risk assessment of the certified EHR technology, and correct identified security deficiencies and provide security updates as part of an ongoing risk management process.*

The EHR Incentive Program and the HIPAA Security Rule do not mandate how the risk analysis and updates should be done. Instead, this is left up to the provider or organization.

Below are commonly recommended steps for performing these tasks:

1. Identify the scope of the analysis
2. Gather data
3. Identify and document potential threats and vulnerabilities
4. Assess current security measures
5. Determine the likelihood of threat occurrence
6. Determine the potential impact of threat occurrence
7. Determine the level of risk
8. Identify security measure and finalize documentation
9. Develop and implement a risk management plan
10. Implement security measures
11. Evaluate and maintain security measures

The risk analysis and risk management process must be conducted at least once prior to the beginning of the EHR reporting period. You will need to attest to CMS or your State that you have conducted this analysis and have taken any corrective action that needs to take place in order to eliminate the security deficiency or deficiencies identified in the risk analysis.

IMPLEMENTATION

MEASUREABLE STEPS

So far, we've covered the legalities of what HHS expects practices to follow and comply with. Now we are going to delve into measurable steps a Physician can implement to ensure their practice meets the requirements of the HIPAA Security Rule.

STEP 1: CONDUCT A THOROUGH RISK ANALYSIS

In order to determine what vulnerabilities are present in your system, practices have to complete an internal risk analysis or have an outside auditor perform one for them. To ensure the risk analysis accurately reflects vulnerabilities, practices have to be willing to admit they are not currently compliant when questioned by an auditor.

As mentioned on page 8, a Risk Analysis must meet NIST standards which include:

- ✓ Identify and document all ePHI repositories
  - This includes all anywhere ePHI may be stored: hard drives, thumb drives, CD's, or removable media
- ✓ Identify and document potential threats and vulnerabilities to each repository
  - Can the data be improperly accessed by unauthorized persons whether internal or external to the practice?
- ✓ Assess current security measures
  - Is access granted according to "minimum necessary" standards? Is the data encrypted?
- ✓ Determine the likeliness of threat occurrence
- ✓ Determine the potential impact of threat occurrence
  - What impact will a privacy breach have on your practice? What impact will a security breach have on your practice?
- ✓ Determine the level of risk

- Based on your current security measures, how likely are you to suffer a data breach?

✓ Determine additional security measures needed to lower level of risk
✓ Document the findings of the Risk Assessment

At a minimum, a risk analysis must be performed annually. However, most practices do not realize that it is also required any time there is a change to the environment (i.e. hiring or firing of personnel, or the acquisition of new equipment that will contain ePHI).

STEP 2: CREATE A REMEDIATION PLAN

It is necessary to take the information from the risk analysis to create a plan to resolve any vulnerabilities that were discovered. In addition to this, practices need to track all documentation showing that all non-compliant issues were resolved. There are some tools that can help practices track the documentation, making the process much easier.

There is no set standard or formula for creating a remediation plan. Each practice will have their own unique problems they uncover during the risk analysis that they need to address.

STEP 3: ENSURE VENDOR COMPLIANCE

Not only does HHS require covered entities to be HIPAA compliant, but under the HITECH Act, Business Associates are required to be compliant as well. This requires your practice to have a valid business associate agreement (BAA) in place with all vendors you do business with that have access to PHI. That means that if your practice has multiple vendors (business associates), for example one that handles billing, another that handles your books, and one that handles your IT needs, you need to have a BAA in place for each and every one.

Further details on Business Associates are provided on page 6.

STEP 4: CREATE A SECURITY COMPLIANCE PLAN

The HIPAA Security Rule requires all covered entities to have a security plan in place. Recently, NIST published a crosswalk utilizing their guidelines for Cybersecurity and matching them to its corresponding requirement under the HIPAA Security Rule. This comprehensive table below does not have to be followed exactly, they are guidelines after all, but you can leverage it to build a complete security plan for your practice.

CATEGORY	SUBCATEGORY	SECURITY RULE
Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(A), 164.310(a)(2)(ii), 164.310(d)
	ID.AM-2: Software platforms and applications within the organization are inventoried	HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(A), 164.308(a)(7)(ii)(E)
	ID.AM-3: Organizational communication and data flows are mapped	HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(A), 164.308(a)(3)(ii)(A), 164.308(a)(8), 164.310(d)
	ID.AM-4: External information systems are catalogued	HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(4)(ii)(A), 164.308(b), 164.314(a)(1), 164.314(a)(2)(i)(B), 164.314(a)(2)(ii), 164.316(b)(2)
	ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	HIPAA Security Rule 45 C.F.R. § 164.308(a)(7)(ii)(E)
	ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(2), 164.308(a)(3), 164.308(a)(4), 164.308(b)(1), 164.314

Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	**ID.BE-1:** The organization's role in the supply chain is identified and communicated	HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(A), 164.308(a)(4)(ii), 164.308(a)(7)(ii)(C), 164.308(a)(7)(ii)(E), 164.308(a)(8), 164.310(a)(2)(i), 164.314, 164.316
	ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(A), 164.308(a)(4)(ii), 164.308(a)(7)(ii)(C), 164.308(a)(7)(ii)(E), 164.308(a)(8), 164.310(a)(2)(i), 164.314, 164.316
	ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(C), 164.308(a)(7)(ii)(D), 164.308(a)(7)(ii)(E), 164.310(a)(2)(i), 164.316
	ID.BE-4: Dependencies and critical functions for delivery of critical services are established	HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(7)(i), 164.308.(a)(7)(ii)(E), 164.310(a)(2)(i), 164.312(a)(2)(ii), 164.314(a)(1), 164.314(b)(2)(i)
	ID.BE-5: Resilience requirements to support delivery of critical services are established	HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(B), 164.308(a)(6)(ii), 164.308(a)(7), 164.308(a)(8), 164.310(a)(2)(i), 164.312(a)(2)(ii), 164.314(b)(2)(i)
	ID.GV-1: Organizational information security policy is established	HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(i), 164.316

Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	**ID.GV-2:** Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(i), 164.308(a)(2), 164.308(a)(3), 164.308(a)(4), 164.308(b), 164.314
	ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	HIPAA Security Rule 45 C.F.R. §§ 164.306, 164.308, 164.310, 164.312, 164.314, 164.316
	ID.GV-4: Governance and risk management processes address cybersecurity risks	HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1), 164.308(b)
Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-1:** Asset vulnerabilities are identified and documented	HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(A), 164.308(a)(7)(ii)(E), 164.308(a)(8), 164.310(a)(1), 164.312(a)(1), 164.316(b)(2)(iii)
	ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources	While performing their HIPAA Security Rule required risk analysis, organizations should consider participating in cyber-threat sharing to reduce their security risk.
	ID.RA-3: Threats, both internal and external, are identified and documented	HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(D), 164.308(a)(3), 164.308(a)(4), 164.308(a)(5)(ii)(A), 164.310(a)(1), 164.310(a)(2)(iii),

		164.312(a)(1), 164.312(c), 164.312(e), 164.314, 164.316
	ID.RA-4: Potential business impacts and likelihoods are identified	HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(i), 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(6), 164.308(a)(7)(ii)(E), 164.308(a)(8), 164.316(a)
	ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(1)(ii)(D), 164.308(a)(7)(ii)(D), 164.308(a)(7)(ii)(E), 164.316(a)
	ID.RA-6: Risk responses are identified and prioritized	HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(B), 164.314(a)(2)(i)(C), 164.314(b)(2)(iv)
Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders	HIPAA Security Rule 45 C.F.R. § 164.308(a)(1)(ii)(B)
	ID.RM-2: Organizational risk tolerance is determined and clearly expressed	HIPAA Security Rule 45 C.F.R. § 164.308(a)(1)(ii)(B)
	ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(B), 164.308(a)(6)(ii), 164.308(a)(7)(i), 164.308(a)(7)(ii)(C),164.308(a)(7)(ii)(E), 164.310(a)(2)(i)

Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are managed for authorized devices and users	HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(3)(ii)(B), 164.308(a)(3)(ii)(C), 164.308(a)(4)(i), 164.308(a)(4)(ii)(B), 164.308(a)(4)(ii)(C), 164.312(a)(2)(i), 164.312(a)(2)(ii), 164.312(a)(2)(iii), 164.312(d)
	PR.AC-2: Physical access to assets is managed and protected	HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(B), 164.308(a)(7)(i), 164.308(a)(7)(ii)(A), 164.310(a)(1), 164.310(a)(2)(i), 164.310(a)(2)(ii), 164.310(a)(2)(iii), 164.310(b), 164.310(c), 164.310(d)(1), 164.310(d)(2)(iii)
	PR.AC-3: Remote access is managed	HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(4)(i), 164.308(b)(1), 164.308(b)(3), 164.310(b), 164.312(e)(1), 164.312(e)(2)(ii)
	PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(3), 164.308(a)(4), 164.310(a)(2)(iii), 164.310(b), 164.312(a)(1), 164.312(a)(2)(i), 164.312(a)(2)(ii)
	PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(4)(ii)(B), 164.310(a)(1), 164.310(b), 164.312(a)(1), 164.312(b), 164.312(c), 164.312(e)

Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security related duties and responsibilities consistent with related policies, procedures, and agreements.	**PR.AT-1:** All users are informed and trained	HIPAA Security Rule 45 C.F.R. § 164.308(a)(5)
	PR.AT-2: Privileged users understand roles & responsibilities	HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(2), 164.308(a)(3)(i), 164.308(a)(5)(i), 164.308(a)(5)(ii)(A), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(5)(ii)(D)
	PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	HIPAA Security Rule 45 C.F.R. §§ 164.308(b), 164.314(a)(1), 164.314(a)(2)(i), 164.314(a)(2)(ii)
	PR.AT-4: Senior executives understand roles & responsibilities	HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(2), 164.308(a)(3)(i), 164.308(a)(5)(i), 164.308(a)(5)(ii)(A), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(5)(ii)(D)
	PR.AT-5: Physical and information security personnel understand roles & responsibilities	HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(2), 164.308(a)(3)(i), 164.308(a)(5)(i), 164.308(a)(5)(ii)(A), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(5)(ii)(D), 164.530(b)(1)
	PR.DS-1: Data-at-rest is protected	HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(b)(1),

Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.		164.310(d), 164.312(a)(1), 164.312(a)(2)(iii), 164.312(a)(2)(iv), 164.312(b), 164.312(c), 164.314(b)(2)(i), 164.312(d)
	PR.DS-2: Data-in-transit is protected	HIPAA Security Rule 45 C.F.R. §§ 164.308(b)(1), 164.308(b)(2), 164.312(e)(1), 164.312(e)(2)(i), 164.312(e)(2)(ii), 164.314(b)(2)(i)
	PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(A), 164.310(a)(2)(ii), 164.310(a)(2)(iii), 164.310(a)(2)(iv), 164.310(d)(1), 164.310(d)(2)
	PR.DS-4: Adequate capacity to ensure availability is maintained	HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(7), 164.310(a)(2)(i), 164.310(d)(2)(iv), 164.312(a)(2)(ii)
	PR.DS-5: Protections against data leaks are implemented	HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(3), 164.308(a)(4), 164.310(b), 164.310(c), 164.312(a), 164.312(e)
	PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.312(b), 164.312(c)(1), 164.312(c)(2), 164.312(e)(2)(i)
	PR.DS-7: The development and testing environment(s)	HIPAA Security Rule 45 C.F.R. § 164.308(a)(4)

	are separate from the production environment	
Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained	HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(8), 164.308(a)(7)(i), 164.308(a)(7)(ii)
	PR.IP-2: A System Development Life Cycle to manage systems is implemented	HIPAA Security Rule 45 C.F.R. § 164.308(a)(1)(i)
	PR.IP-3: Configuration change control processes are in place	HIPAA Security Rule 45 C.F.R. § 164.308(a)(8)
	PR.IP-4: Backups of information are conducted, maintained, and tested periodically	HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(7)(ii)(A), 164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(D), 164.310(a)(2)(i), 164.310(d)(2)(iv)
	PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(7)(i), 164.308(a)(7)(ii)(C), 164.310, 164.316(b)(2)(iii)
	PR.IP-6: Data is destroyed according to policy	HIPAA Security Rule 45 C.F.R. §§ 164.310(d)(2)(i), 164.310(d)(2)(ii)

	PR.IP-7: Protection processes are continuously improved	HIPAA Security Rule 45 C.F.R. §§ 164.306(e), 164.308(a)(7)(ii)(D), 164.308(a)(8), 164.316(b)(2)(iii)
	PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties	HIPAA Security Rule 45 C.F.R. § 164.308(a)(6)(ii)
	PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(6), 164.308(a)(7), 164.310(a)(2)(i), 164.312(a)(2)(ii)
	PR.IP-10: Response and recovery plans are tested	HIPAA Security Rule 45 C.F.R. § 164.308(a)(7)(ii)(D)
	PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(C), 164.308(a)(3)
	PR.IP-12: A vulnerability management plan is developed and implemented	HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(i), 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B)

Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.	**PR.MA-1:** Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(3)(ii)(A), 164.310(a)(2)(iv)
	PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(3)(ii)(A), 164.310(d)(1), 164.310(d)(2)(ii), 164.310(d)(2)(iii), 164.312(a), 164.312(a)(2)(ii), 164.312(a)(2)(iv), 164.312(b), 164.312(d), 164.312(e), 164.308(a)(1)(ii)(D)
Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(C), 164.310(a)(2)(iv), 164.310(d)(2)(iii), 164.312(b)
	PR.PT-2: Removable media is protected and its use restricted according to policy	HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(3)(i), 164.308(a)(3)(ii)(A), 164.310(d)(1), 164.310(d)(2), 164.312(a)(1), 164.312(a)(2)(iv), 164.312(b)
	PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(3), 164.308(a)(4), 164.310(a)(2)(iii), 164.310(b), 164.310(c), 164.312(a)(1), 164.312(a)(2)(i), 164.312(a)(2)(ii), 164.312(a)(2)(iv)
	PR.PT-4: Communications and control networks are protected	HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.312(a)(1), 164.312(b), 164.312(e)

Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood.	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed	HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.312(b)
	DE.AE-2: Detected events are analyzed to understand attack targets and methods	HIPAA Security Rule 45 C.F.R. § 164.308(6)(i)
	DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(6)(ii), 164.308(a)(8), 164.310(d)(2)(iii), 164.312(b), 164.314(a)(2)(i)(C), 164.314(a)(2)(iii)
	DE.AE-4: Impact of events is determined	HIPAA Security Rule 45 C.F.R. § 164.308(a)(6)(ii)
	DE.AE-5: Incident alert thresholds are established	HIPAA Security Rule 45 C.F.R. § 164.308(a)(6)(i)
	DE.CM-1: The network is monitored to detect potential cybersecurity events	HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(8), 164.312(b), 164.312(e)(2)(i)

Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-2:** The physical environment is monitored to detect potential cybersecurity events	HIPAA Security Rule 45 C.F.R. §§ 164.310(a)(2)(ii), 164.310(a)(2)(iii)
	DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(3)(ii)(A), 164.308(a)(5)(ii)(C), 164.312(a)(2)(i), 164.312(b), 164.312(d), 164.312(e)
	DE.CM-4: Malicious code is detected	HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B)
	DE.CM-5: Unauthorized mobile code is detected	HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B)
	DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	HIPAA Security Rule 45 C.F.R. § 164.308(a)(1)(ii)(D)
	DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.310(a)(1), 164.310(a)(2)(ii), 164.310(a)(2)(iii), 164.310(b), 164.310(c), 164.310(d)(1), 164.310(d)(2)(iii), 164.312(b), 164.314(b)(2)(i)

	DE.CM-8: Vulnerability scans are performed	HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(i), 164.308(a)(8)
Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	**DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability	HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(2), 164.308(a)(3)(ii)(A), 164.308(a)(3)(ii)(B), 164.308(a)(4), 164.310(a)(2)(iii), 164.312(a)(1), 164.312(a)(2)(ii)
	DE.DP-2: Detection activities comply with all applicable requirements	HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(i), 164.308(a)(8)
	DE.DP-3: Detection processes are tested	HIPAA Security Rule 45 C.F.R. § 164.306(e)
	DE.DP-4: Event detection information is communicated to appropriate parties	HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(6)(ii), 164.314(a)(2)(i)(C), 164.314(a)(2)(iii)
	DE.DP-5: Detection processes are continuously improved	HIPAA Security Rule 45 C.F.R. §§ 164.306(e), 164.308(a)(8)
Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.	**RS.RP-1:** Response plan is executed during or after an event	HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(6)(ii), 164.308(a)(7)(i), 164.308(a)(7)(ii)(A), 164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(C), 164.310(a)(2)(i), 164.312(a)(2)(ii)

Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	**RS.CO-1:** Personnel know their roles and order of operations when a response is needed	HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(2), 164.308(a)(7)(ii)(A), 164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(C), 164.310(a)(2)(i), 164.308(a)(6)(i), 164.312(a)(2)(ii)
	RS.CO-2: Events are reported consistent with established criteria	HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(6)(ii), 164.314(a)(2)(i)(C), 164.314(a)(2)(iii)
	RS.CO-3: Information is shared consistent with response plans	HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(6)(ii), 164.314(a)(2)(i)(C)
	RS.CO-4: Coordination with stakeholders occurs consistent with response plans	HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(6), 164.308(a)(7), 164.310(a)(2)(i), 164.312(a)(2)(ii)
	RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	HIPAA Security Rule 45 C.F.R. § 164.308(a)(6)
	RS.AN-1: Notifications from detection systems are investigated	HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(i), 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(6)(ii), 164.312(b)

Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.	**RS.AN-2:** The impact of the incident is understood	HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(6)(ii), 164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(C), 164.308(a)(7)(ii)(E)
	RS.AN-3: Forensics are performed	HIPAA Security Rule 45 C.F.R. § 164.308(a)(6)
	RS.AN-4: Incidents are categorized consistent with response plans	HIPAA Security Rule 45 C.F.R. § 164.308(a)(6)(ii)
Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	**RS.MI-1:** Incidents are contained	HIPAA Security Rule 45 C.F.R. § 164.308(a)(6)(ii)
	RS.MI-2: Incidents are mitigated	HIPAA Security Rule 45 C.F.R. § 164.308(a)(6)(ii)
	RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(6)(ii)
Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	**RS.IM-1:** Response plans incorporate lessons learned	HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(7)(ii)(D), 164.308(a)(8), 164.316(b)(2)(iii))
	RS.IM-2: Response strategies are updated	HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(7)(ii)(D), 164.308(a)(8)

Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	**RC.RP-1:** Recovery plan is executed during or after an event	HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(7), 164.310(a)(2)(i)
Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	**RC.IM-1:** Recovery plans incorporate lessons learned	HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(7)(ii)(D), 164.308(a)(8), 164.316(b)(2)(iii)
	RC.IM-2: Recovery strategies are updated	HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(7)(ii)(D), 164.308(a)(8)
Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.	**RC.CO-1:** Public relations are managed	Although public relations management and reputation repair are not specifically required by the HIPAA Security Rule's Security Incident Procedures standard (45 C.F.R. § 164.308(a)(6)(i)), HIPAA covered entities and business associates may implement such procedures as components of their compliance activities.
	RC.CO-2: Reputation after an event is repaired	Although public relations management and reputation repair are not specifically required by the HIPAA Security Rule's Security

		Incident Procedures standard (45 C.F.R. § 164.308(a)(6)(i)), HIPAA covered entities and business associates may implement such procedures as components of their compliance activities.
	RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams	HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(6)(ii), 164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(C), 164.310(a)(2)(i), 164.314(a)(2)(i)(C)

STEP 5: PROTECTING EPHI

Now that a plan has been established it is up to you, to ensure it is implemented. Unless you have a strong technical background, the first question you'll ask is "How?" It's important to remember that when it comes to security, you cannot just look at one point of failure, one vulnerability, secure it, and think you're all set. The real key to security is looking across the entire spectrum, thinking of it from a holistic perspective, and analyzing and securing each vulnerability as much as possible.

The areas you need to look at include:

- Securing the Network Gateway with a UTM device
  - This is also known as a Next-Generation Firewall which includes many advanced features to block current threats
- SPAM & Phishing Filtering & Blocking
- Data Loss Prevention
- Continuous Security Monitoring
- Threat Response
  - If a breach is discovered, it is essential to respond as quickly as possible to mitigate any damage that was caused
- Anti-Virus / Anti-Malware Protection for each connected device
- Data Encryption

- Encrypting Data Transmissions
  - This includes fax, email, and text messaging
- Mobile Device Security
  - If tablets or phones are used to access PHI or the network, you need to make sure they are secure
- Patch Management
  - Microsoft is always putting out updated patches to fix security flaws
- Software Updates
  - Unpatched software can be exploited and leave your practice vulnerable
- Daily & Weekly Backups
  - It's good to have backups, but they should be periodically tested to ensure you can recover the data
- Disaster Recovery Planning
  - As ransomware is increasingly targeting healthcare, it has become essential to have a disaster recovery plan in place
- Password Management
  - Sharing passwords or writing them down on sticky notes is often common practice, but if those passwords grant access to ePHI, it becomes a HIPAA violation and can turn into a major problem

STEP 6: COMPLIANCE TRAINING & TESTING

One of the most important steps you can take to protect e-PHI and patient information is to provide security training for each member of your staff. The human element is always going to be the weakest link in the chain. People make mistakes, its part of life. The best way you can mitigate that risk is by ensuring everyone is well-trained.

Your practice should provide for in-depth training on the HIPAA Security Rule as well as best practices in protecting PHI and patient information. Some of the topics covered in the training should include:

- What is considered PHI?
- What does the HIPAA Security Rule cover?

- How to Protect PHI
- Protecting Passwords
- Auditing ePHI
- Recognizing and Preventing Malware
- Using Encryption to protect ePHI
- Security Breaches and Violations
- Practical Security Steps

Once your staff has completed the training, they should be tested, and a report should be maintained that lists each staff member, and the date they took the training.

STEP 7: PROPER DOCUMENTATION

The HIPAA omnibus rule requires practices to have a manual containing all policies and procedures that address each aspect of the omnibus rule, such as business associate agreements, access control, and security plans. However, it is not enough to simply have policies and procedures, HHS requires that they be current and up to date. It is recommended that your policies and procedures be reviewed annually during your Risk Analysis to ensure they are current.

STEP 8: ROUTINE ASSESSMENTS

It is important to ensure that your organization's policies and procedures are being followed. If they only exist on paper, but aren't routinely followed, they are completely useless. Worse, when your practice suffers a data breach and OCR conducts their investigation, they may decide to levy a fine for "willful negligence" and your practice will be on the hook for millions of dollars – which is typically not covered by liability insurance.

Routine testing, in the form of vulnerability assessments, penetration testing (if you support a large practice), and security audits will go a long way towards ensuring compliance. These are typically standard practice with large organizations, but that does not preclude your practice from leveraging the same methodology.

In conclusion, your focus should not be solely on compliance, but on protecting the patients. Identity theft is very common in a healthcare data breach, and has ruined many lives.

BREACH NOTIFICATION

The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires practices and their business associates to notify HHS following a breach of unsecured PHI. The Federal Trade Commission (FTC), has similar breach notification provisions that they enforce, and applies to vendors of personal health records and their third party providers, under section 13407 of the HITECH Act.

BREACH DEFINITION

HHS generally defines a breach as *an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information.* Any authorized use or disclosure of PHI should be treated as a breach unless your practice can demonstrate otherwise.

HHS recommends practices conduct a risk assessment after a breach that consists of the following factors:

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

EXCEPTIONS

HHS allows for three exceptions to what may be considered a “breach.” The first exception allows for unintentional disclosure of PHI from someone authorized to access it to another person at the same location (or a business associate) with a general authority to view or access PHI, it is not considered a breach.

The second exception allows for inadvertent disclosure of PHI from someone authorized to access it to another person at the same location (or a business associate) with a general authority to view or access PHI, it is not considered a breach, so long as the information cannot be used or disclosed in a way not permitted under the Privacy Rule.

The final exception applies if the practice or business associate who disclosed PHI believes that the person who received the information would quickly forget about it.

WHEN TO REPORT A BREACH

HHS states that: *covered entities and business associates must only provide the required notifications if the breach involved unsecured protected health information. Unsecured protected health information is protected health information that has not been rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology.*

In other words, a practice only needs to report a breach if the PHI was not secure (i.e. unencrypted). If a practice has a data breach, but the PHI was encrypted, it does not need to be reported.

BREACH NOTIFICATION REQUIREMENTS

After a practice suffers a data breach that includes unsecured PHI, they must notify the people affected, the Secretary of HHS, and, in certain cases, the media as well. Additionally, if a business associate experiences a breach they must notify the practice they support.

INDIVIDUAL NOTICE

Practices are required to notify all individuals whose private health information was compromised in a data breach. They are required to do this by sending a written notice, or email if that person has opted for that mode of communication. If the contact information for 10 or more of the affected individuals is out-of-date, then the practice must post a notice on the home page of its website for 90 days or provide a media notice in the town where the individuals live. Additionally, practices must include a toll-free number that is active for 90 days, so that individuals can call and find out if their information was compromised in the breach.

Practices have up till 60 days after a breach has been discovered to send out notifications to all individuals affected. Details have to include the following:

- A description of the breach
- Types of information involved
- Steps the person can take to protect their identity
- Steps the practice is taking to investigate the breach
- Steps the practice is taking to mitigate the damage
- Steps the practice is taking to prevent future breaches
- Contact information for the practice

MEDIA NOTICE

Practices that experience a data breach that impacts more than 500 residents of a particular State are required to contact the media in that State and notify them of the breach. HHS recommends this be done in the form of a press release to the local news media in the area. As with the individual notice, the media notice must be released within 60 days after a practice discovers the breach and must include the same information provided in the notice sent out to individuals.

NOTICE TO THE SECRETARY

In addition to notifying the individuals impacted, and the media (in cases involving more than 500 individuals), practices are required to notify the Secretary of HHS any time they discover a data breach - no matter how big or small. If a breach impacted 500 or more individuals, a practice has up to 60 days after they discover the breach to report it. If a breach affected less than 500 people, a practice has until 60 days after the end of the calendar year to report it.

All reports to HHS must be made online. The link can be found here:

http://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html

BREACH OF A BUSINESS ASSOCIATE

If a business associate experiences a data breach, the business associate is required to notify the practice after they discover the breach. They have up to 60 days after they discover the breach to report it to the practice. The business associate should provide the practice with the identity of each individual impacted by the breach, as well as any other information the practice may require.

If a business associate suffers a data breach, although the practice is responsible for notifying all impacted individuals, they can delegate that responsibility to the business associate. This is typically best determined by deciding which entity has more of a direct relationship with the persons impacted.

BURDEN OF PROOF

When either a practice or a business associate suffers a data breach, they have to provide HHS with proof that they have done their due diligence. They need to provide documentation that all notifications were made to all relevant parties, or that the unauthorized use or disclosure of PHI did not constitute a breach (see Exceptions, pg. 34). If either a practice or a business associate determined that notification was not required they need to submit a risk assessment demonstrating that PHI has not been compromised, or that the unauthorized use of PHI meets the requirements for an exception (pg.34).

As part of the Administrative Safeguards, practices and business associates must have documented policies and procedures implemented regarding breach notification. All staff must be trained on these policies and procedures, and penalties must be imposed against staff whom are non-compliant.

Each report has to be submitted via a web portal through HHS by going to this link: http://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html

Each State and Territory have their own breach notification requirements, be sure to check with your Attorney General to determine your local responsibilities.

NON-COMPLIANCE

HIPAA / HITECH PENALTIES

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) established rules protecting the privacy and security of individually identifiable health information.

Failure to comply with HIPAA requirements can result in civil and criminal penalties, as well as progressive disciplinary actions through your organization, up to and including termination. These civil and criminal penalties can apply to both covered entities and individuals.

Section 13410(D) of the HITECH Act, which became effective on February 18, 2009, revised section 1176(a) of the Social Security Act by establishing:

- Four categories of violations that reflect increasing levels of culpability
- Four corresponding tiers of penalties that significantly increase the minimum penalty amount for each violation
- A maximum penalty amount of $1.5 million for all violations of an identical provision

See the table below for further details:

Civil Penalties	
Tier	**Penalty**
1. Covered entity or individual did not know (and by exercising reasonable diligence would not have known) the act was a HIPAA violation.	$100-$50,000 for each violation, up to a maximum of $1.5 million for identical provisions during a calendar year

2. The HIPAA violation had a reasonable cause and was not due to willful neglect.	$1,000-$50,000 for each violation, up to a maximum of $1.5 million for identical provisions during a calendar year
3. The HIPAA violation was due to willful neglect but the violation was corrected within the required time period.	$10,000-$50,000 for each violation, up to a maximum of $1.5 million for identical provisions during a calendar year
4. The HIPAA violation was due to willful neglect and was not corrected.	$50,000 or more for each violation, up to a maximum of $1.5 million for identical provisions during a calendar year
Criminal Penalties	
Tier	**Potential Jail Sentence**
Unknowingly or with reasonable cause	Up to one year
Under false pretenses	Up to five years
For personal gain or malicious reasons	Up to ten years

ENFORCEMENT

HHS' Office for Civil Rights (OCR) is responsible for enforcing the Privacy and Security Rules *(45 C.F.R. Parts 160 and 164, Subparts A, C, and E).*

Enforcement of the Privacy Rule began April 14, 2003. The Security Rule has been enforced by OCR since 2009, and the Omnibus Rule has been enforced since 2013.

OCR carries out its mandate in three ways. They include:

- Investigating complaints
- Performing random audits
- Education & Outreach

COMPLAINT REVIEW

OCR is careful to review all complaints they receive. As required by law, they can only act on complaints that meet the following criteria:

- The alleged violation must have taken place after the Rules took effect.
    - April 14, 2003 for the Privacy Rule
    - April 20, 2005 for the Security Rule
    - January 25, 2013 for the Omnibus Rule
- The complaint must be filed against an organization that is required to comply with the Privacy & Security Rules.
    - Covered Entities - includes:
        - Hospitals
        - Clinics
        - Doctors
        - Dentists

        - Psychologists
        - Chiropractors
        - Physical Therapists
    - Business Associates - can include
        - Third-party billing agencies
        - Lawyers
        - CPA's
        - Health Insurance Providers
        - Health Care Plans – Public & Private
        - IT Service Providers
- The person filing the complaint must allege that the Privacy or Security Rules were violated.
- Complaints must be filed within 180 days of when the person knew about the alleged violation of either the Privacy Rule or the Security Rule.
    - OCR can grant an exception if proof can be furnished that submitting a complaint within this timeframe was impossible

Some organizations are granted compliance exemptions from the Privacy and Security Rules in specific circumstances. They include:

- Life Insurers
- Employers
- Workers Compensation Carriers
- Most Schools and School Districts
- Some State Agencies, like Child Protective Services
- Most Law Enforcement Agencies
- Many Municipal Offices

INVESTIGATING A COMPLAINT

If a complaint is accepted for investigation, OCR will send out a notification both to the person who filed the complaint, as well as the organization named in it. Next, the individual who filed the complaint and the organization are required to provide evidence regarding the issue described in the complaint. OCR may then request further information from both parties to gain a better understanding of the facts. If the complaint involves a criminal violation of HIPAA under 42 USC 1320d-6, the complaint will likely be referred to the Department of Justice for further investigation.

NON-COMPLIANCE RESOLUTION

It is OCR's responsibility to review all the evidence that it gathers in each case. On rare occasion, it may make the determination that the organization violated neither the Privacy nor the Security Rule. However, if the evidence shows that the organization was not in compliance, OCR attempts to resolve the case in three ways:

Voluntary Compliance
Corrective Action
Resolution Agreement

Once a resolution has been obtained, a written notification is sent both to the person who filed the complaint and the organization.

If OCR determines that the organization did not satisfactorily resolve the matter, they can impose civil monetary penalties (CMPs). In this case, the organization reserves the right to request a formal hearing overseen by an HHS administrative law judge. The judge will then decide if the penalties are supported by the evidence. Any monies awarded in these cases are the property of the U.S. Treasury.

Currently, OCR is enforcing the most recent legislation, known as the Omnibus Rule which made significant changes to the Privacy & Security Rules.

For a full text of the rule go here:
http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf

For a summary by American Health Management Association (AHIMA) go here:
http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_050067.pdf

ENFORCEMENT CASE STUDIES

HHS Office of the Inspector General (OIG) recently published two reports demanding that the Office of Civil Rights (OCR) take immediate action to strengthen their oversight and enforcement of HIPAA compliance. Following this, the director of OCR, Jocelyn Samuels, has levied harsher fines and implemented stricter enforcement of HIPAA violations. Additionally, OCR also announced that they are planning to implement a permanent audit program.

$1.5 MILLION FINE FOR LACK OF BAA

On March 16, 2016, The Department of Health and Human Services' Office for Civil Rights announced it has reached a settlement with North Memorial Health Care of Minnesota over HIPAA violations from a 2011 data breach. North Memorial has agreed to pay a $1,550,000 fine to OCR to settle the HIPAA violation charges.

Following a breach reported on September 27, 2011, OCR conducted an investigation and discovered HIPAA violations that contributed to the cause of a breach of 9,497 patient health records. The investigation revealed that North Memorial had overlooked "Two major cornerstones of the HIPAA Rules," according to OCR Director Jocelyn Samuels.

The data breach involved the theft of a laptop computer from a business associate of North Memorial. The laptop was stolen from the employee's vehicle, and while the device was password-protected, the ePHI stored on the device had not been encrypted.

Prior to access to patient data being granted, North Memorial had not obtained a signed copy of a HIPAA-compliant business associate agreement (BAA).

Under HIPAA Rules, covered entities must obtain a signed BAA from any vendor that provides functions, activities or services for or on behalf of a covered entity that requires access to patient ePHI. A signed copy of the BAA must be obtained before access to patient health data is provided. The BAA must outline the responsibilities the business

associate has to ensure PHI is protected and is not disclosed to any unauthorized parties.

The investigation also revealed that North Memorial had not performed a comprehensive risk analysis for the entire organization. Consequently, North Memorial would not have been able to identify all security vulnerabilities and could therefore not have taken action to address all issues.

A HIPAA risk analysis must cover "*all applications, software, databases, servers, workstations, mobile devices and electronic media, network administration and security devices, and associated business processes*," according to OCR.

In a press release issued on March 16, Samuels said "*Organizations must have in place compliant business associate agreements as well as an accurate and thorough risk analysis that addresses their enterprise-wide IT infrastructure."*

$750,000 FINE FOR LACK OF PROPER RISK ANALYSIS

On September 2, 2015 The HHS Office of Civil Rights (OCR) issued a press release announcing a $750,000 HIPAA settlement with Cancer Care Group, P.C.

On August 29, 2012, OCR received notification from Cancer Care regarding a breach of unsecured electronic protected health information (ePHI) after a laptop bag was stolen from an employee's car. The bag contained the employee's computer and unencrypted backup media, which contained the names, addresses, dates of birth, Social Security numbers, insurance information and clinical information of approximately 55,000 current and former Cancer Care patients.

OCR's subsequent investigation found that, prior to the breach, Cancer Care was in widespread non-compliance with the HIPAA Security Rule. It had not conducted an enterprise-wide risk analysis when the breach occurred in July 2012. Further, Cancer Care did not have in place a written policy specific to the removal of hardware and electronic media containing ePHI into and out of its facilities, even though this was common practice within the organization. OCR found that these two issues, in particular, contributed to the breach, as an enterprise-wide risk analysis could have identified the removal of unencrypted backup media as an area of significant risk to Cancer Care's ePHI, and a comprehensive device and media control policy could have provided employees with direction in regard to their responsibilities when removing devices containing ePHI from the facility.

"*Organizations must complete a comprehensive risk analysis and establish strong policies and procedures to protect patients' health information," said OCR Director Jocelyn Samuels. "Further, proper encryption of mobile devices and electronic media reduces the likelihood of a breach of protected health information*."

Most liability insurance policies DO NOT cover HIPAA related fines. In most cases these expenses have to be paid out of pocket.

FOR MORE INFORMATION:

CONTACT VITECH TO LEARN HOW WE CAN HELP YOUR PRACTICE WITH HIPAA COMPLIANCE.

PHONE: 800-536-2156

EMAIL: hipaa@vitechpros.com

WEB: VITECHPROS.COM

[i] Sources:
http://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html
http://www.hhs.gov/hipaa/for-professionals/privacy/index.html
http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf
http://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html
https://www.healthit.gov/providers-professionals/meaningful-use-definition-objectives
http://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html
http://www.hhs.gov/sites/default/files/NIST%20CSF%20to%20HIPAA%20Security%20Rule%20Crosswalk%2002-22-2016%20Final.pdf
http://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/
http://www.hhs.gov/hipaa/for-professionals/special-topics/HITECH-act-enforcement-interim-final-rule/index.html