**The Health Insurance Portability and Accountability Act of 1996 (HIPAA)**

**Best Practices and Helpful Information**

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) required the Secretary of the U.S. Department of Health and Human Services (HHS) to develop regulations protecting the privacy and security of certain health information.

**10 HIPAA Compliance Best Practices**

1. **Encrypt health information**

Healthcare data encryption is when organizations convert data into encoded text, which makes the information unreadable unless a user has a key or code to decrypt it. This could be a good option for covered entities or business associates that regularly handle electronic PHI (ePHI), and want to ensure that unauthorized users cannot access the data.

* Among many worrying insights, we found between 2009 and 2019:
  + 3,054 data breaches of healthcare records
  + 230,954,151 healthcare records lost, stolen, or exposed
  + 70% of the US population affected by healthcare data breaches
* The effect of COVID-19 on individuals, businesses, and the entire world with these revealing 2020 [cybersecurity](https://www.pandasecurity.com/en-us/homeusers/) statistics.
  + COVID-19 can already be classified as the largest-ever cybersecurity threat.
  + Cyber-attacks were most prevalent in the healthcare and financial industries.
  + [Email phishing attacks](https://www.pandasecurity.com/en/mediacenter/tips/stop-spam-emails/) were the most common source of data breaches while working from home.
  + Amongst the heightened security threats, [organizational cybersecurity](https://www.pandasecurity.com/en/mediacenter/news/what-is-cyber-resilience/) budgets are still expected to decrease in 2021.

1. **Assess your risk**

Conduct a complete [risk assessment](https://www.securitymetrics.com/guided-hipaa) of all the elements of your ecosystem that store, process, or transfer electronic PHI (ePHI). Make sure to evaluate the ways in which your information could be exposed. If your environment includes a data center, you should ask these questions:

* Are natural disasters common in the location of the data center?
* Is there a responsible party associated with all hardware components?
* Have you assessed the security mechanisms that are now in place and any risks that are present?
* Have you taken into account all ways in which ePHI is accessed or manipulated within your system? (Consider the creation, receipt, maintenance, and transfer of ePHI).

1. **Setup passwords or authentication requirements for software applications and devices**

Ensure that staff members are using strong passwords that should include complexity and length (including numbers and special characters).

1. **Do not entertain gossip within the organization**

Ensure that staff members understand what is at stake if they reveal patient health information to an unauthorized person.

1. **Training is fundamental! Properly train staff regarding HIPAA**

Ensure staff members are trained to be suspicious of emails that ask the user to click a link or ask for sensitive information. If a staff member clicks on a link or submits data—like a username or a social security number—they essentially hand over the keys to your organization’s data environment. It’s scary but true that something as simple as a fake email could create a point of entry for attackers to exploit. Keep in mind that no matter how extensive your training program is, people make mistakes. Back up your training program with technical security controls that prevent employees from installing malware or visiting spoofed websites.

1. **Put incident response plans into place**

Staff members should test the plan so all know and understand their role and responsibilities

1. **Be Vigilant and ready to act**

Although not fun to think about, it's critical to [be prepared](http://info.securitymetrics.com/effectively-manage-a-healthcare-data-breach) for the possibility of a breach. You need a planned response that is easy to execute, but thoroughly designed. The Office for Civil Rights’ [checklist](https://www.hhs.gov/sites/default/files/cyber-attack-checklist-06-2017.pdf) lists the steps of a proper response after a breach of HIPAA-protected material:

1. Carry out your response and mitigation steps.
2. Stop the attack and contain the threat to privacy and security.
3. Report the incident to law enforcement.
4. Submit the relevant cyber threat indicators to federal and information sharing and analysis organizations (ISAOs).
5. Notify the Office for Civil Rights quickly, within 60 days following the detection of a breach that compromised at least 500 people.
6. **Be vigilant about third-party business agreements**

When considering a new relationship with a vendor, it is necessary to inquire whether they perform a security risk analysis of their information systems and how they handle PHI. Understand how the contract with the vendor will protect PHI. In addition, if the third-party vendor has designated a privacy and security officer and what type of training is given to their employees.

1. **Avoid improper PHI disclosure**

Use extreme care and ensure that information is not getting into the wrong hands. Use care when sending emails and make sure it does not contain PHI/ePHI or mixing up name and patient ID information. This could result in an unauthorized individual gaining access to patient health information.

1. **Designate a HIPPA champion**

Designate and empower an individual or a leader in your organization to review, evaluate, and investigate your organization’s HIPAA compliance efforts

**Top 10 Most common HIPAA Violations**

1. **Keeping Unsecured Records**

As part of your employee training, all staff members should be required to keep documents with PHI in a secure location at all times. Physical files containing PHI should be locked in a desk, filing cabinet or office. Digital files should require secure passwords to access them, in addition to being encrypted whenever possible.

1. **Unencrypted Date**

The dangers of leaving PHI data vulnerable without encryption are simple. Encrypting the data is an added protection if a device containing PHI is lost or stolen. It offers an additional layer of security if a password protected device is somehow accessed, such as through hacking. Although it is not a strict HIPAA requirement, it is highly recommended. You should also be familiar with your State HIPAA regulations as many States have passed laws requiring ePHI and PII to be encrypted.

1. **Hacking**

Although we'd like to think it would never happen to us, hacking is a real threat to medical ePHI. There are people out there who want to use this information for malicious purposes, and therefore medical practices need to protect against hacking wherever possible.

Keeping antivirus software updated and active on all devices containing ePHI is a great place to start. Using firewalls adds another layer of protection as well. Finally, creating unique and difficult to remember passwords, and changing them frequently is another important measure to take to prevent hacking.

1. **Loss or Theft of Devices**

A case was settled in June of 2016, where an iPhone containing a vast amount of ePHI, including social security numbers, treatment and diagnosis information, medications, and more was stolen.

In addition, the iPhone was neither password protected nor encrypted, leaving all ePHI vulnerable to access by anyone possessing the phone.

The violation occurred at a facility called the Catholic Health Care Services of the Archdiocese of Philadelphia (CHCS). A combination of nursing home residents and family members totaling 412 people were affected by the data breach, and the facility was fined $650,000.

Unfortunately, if devices containing ePHI are not stored in a secure location at all times, they are subject to the possibility of loss or theft. If the information stored on such devices is not encrypted or password protected, the loss or theft of the device becomes an even more severe issue.

1. **Lack of Employee Training**

When it comes to training employees on HIPAA regulations and compliance, it's important that every employee who comes in contact with PHI be thoroughly educated. Employee HIPAA training is more than a recommendation - it is a requirement of the HIPAA law. All staff members must be well-trained on the law, as well as on the particular policies and procedures set forth by your individual practice.

1. **Gossiping / Sharing PHI**

Although general gossip or chit chat by the water cooler can be harmless, PHI should always be off limits. When talking to co-workers, there is no reason to discuss PHI. Plus, it comes with a hefty fine.

Medical practice employees with access to patient PHI need to be careful about the information they share with others. When discussing PHI, should always be aware of who may be listening. Keep conversations about PHI behind closed doors, and only with appropriate office personnel.

1. **Employee Dishonesty**

Although not always done with a malicious purpose, when employees try to access PHI that they are not authorized to view, this is a HIPAA violation. Often it is merely out of curiosity, but the punishment is the same regardless of the intent. Thorough and precise training and procedures that outline who can access what, as well as a clear indication of the consequences that will result, can help prevent occurrences of this particular HIPAA violation.

1. **Improper Disposal of Records**

When training your staff members on HIPAA regulations, one of the most important procedures to enforce is proper disposal of PHI records. Staff members should understand that all information that contains PHI, such as social security numbers, medical procedures, diagnoses, etc., should be shredded, destroyed, wiped from the hard drive, etc.

If any of this information is left lying around in a trash can, in a computer's recent files folder, etc., it could get into the hands of the wrong person, and this would be a serious HIPAA violation. You can prevent this from happening with proper employee training and enforcement by a compliance officer or other staff.

1. **Unauthorized Release of Information**

This violation most often occurs when members of the media release PHI regarding public figures and celebrities. It can also happen when medical personnel release PHI to family members that are unauthorized, as only dependents and those with a Power of Attorney are allowed access to the PHI of a family member.

1. **3rd Party Disclosure of PHI**

When it comes to discussing PHI, it should only be discussed with the people who need to know, such as the patient, the doctor(s), and/or the person(s) billing for the procedure, medication, or other related service. If you have access to PHI and discuss it with those who do not have the right access to this information is a direct violation of HIPAA.

However, it does happen frequently. Again, by educating all staff members with access to PHI about HIPAA regulations such as this, you can eliminate the majority of data breaches caused by this violation.

Another example of 3rd party disclosure would be if a staff member were to release the wrong patient's information due to human error. In this case, the act may be an accident, but the consequences would be similar to those for a purposeful violation.

**7 says to solve your HIPAA Problems**

1. Implementing policies, procedures and standards of conduct
2. Designating a compliance officer and compliance committee
   1. Compliance Officer addresses the Privacy, Security and Compliance Concerns
3. Conducting effective training and education
4. Developing effective lines of communication
   1. Communication between Compliance Officer and other members of the organization
   2. Communication is Key!
5. Conducting internal monitoring and auditing
   1. Auditing used to ensure policies and procedures are effective to the organization
6. Enforcing standards through well-publicized disciplinary guidelines
7. Responding promptly to detected offenses and undertaking corrective action

**The Security Rule**

The HIPAA Security Rule establishes national standards to protect individuals’ electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.

##### **Administrative Safeguards**

##### **Security Management Process**. A covered entity must identify and analyze potential risks to e-PHI, and it must implement security measures that reduce risks and vulnerabilities to a reasonable and appropriate level.

##### **Security Personnel.** A covered entity must designate a security official who is responsible for developing and implementing its security policies and procedures.

##### **Information Access Management.** Consistent with the Privacy Rule standard limiting uses and disclosures of PHI to the "minimum necessary," the Security Rule requires a covered entity to implement policies and procedures for authorizing access to e-PHI only when such access is appropriate based on the user or recipient's role (role-based access).

##### **Workforce Training and Management.** A covered entity must provide for appropriate authorization and supervision of workforce members who work with e-PHI. A covered entity must train all workforce members regarding its security policies and procedures,and must have and apply appropriate sanctions against workforce members who violate its policies and procedures.

##### **Evaluation**. A covered entity must perform a periodic assessment of how well its security policies and procedures meet the requirements of the Security Rule.

##### **Physical Safeguards**

##### **Facility Access and Control.** A covered entity must limit physical access to its facilities while ensuring that authorized access is allowed.

##### **Workstation and Device Security.** A covered entity must implement policies and procedures to specify proper use of and access to workstations and electronic media. A covered entity also must have in place policies and procedures regarding the transfer, removal, disposal, and re-use of electronic media, to ensure appropriate protection of electronic protected health information (e-PHI).

##### **Technical Safeguards**

##### **Access Control.** A covered entity must implement technical policies and procedures that allow only authorized persons to access electronic protected health information (e-PHI).

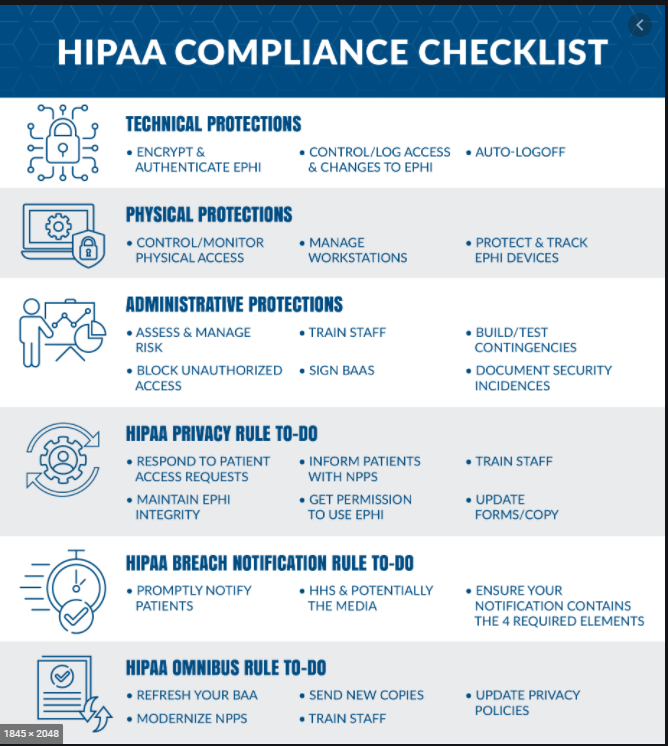
##### **Audit Controls.** A covered entity must implement hardware, software, and/or procedural mechanisms to record and examine access and other activity in information systems that contain or use e-PHI.

##### **Integrity Controls.** A covered entity must implement policies and procedures to ensure that e-PHI is not improperly altered or destroyed. Electronic measures must be put in place to confirm that e-PHI has not been improperly altered or destroyed.

##### **Transmission Security.** A covered entity must implement technical security measures that guard against unauthorized access to e-PHI that is being transmitted over an electronic network.

**HIPAA Compliance Checklist Examples**

<file:///C:/Users/Nicole/Downloads/HIPAAComplianceChecklistDownload.pdf>



**HIPPA Security Rule ToolKit**

The NIST HIPAA Security Toolkit Application is intended to help organizations better understand the requirements of the HIPAA Security Rule, implement those requirements, and assess those implementations in their operational environment. Target users include, but are not limited to, HIPAA covered entities, business associates, and other organizations such as those providing HIPAA Security Rule implementation, assessment, and compliance services. Target user organizations can range in size from large nationwide health plans with vast information technology (IT) resources to small health care providers with limited access to IT expertise.

[NIST\_HSR\_Toolkit\_User\_Guide.pdf](https://csrc.nist.gov/CSRC/media/Projects/Security-Content-Automation-Protocol/HIPPA/NIST_HSR_Toolkit_User_Guide.pdf)

**Sources:**

<https://www.hipaasecurenow.com/index.php/beckers-hipaa-compliance-8-best-practices/>

[5 Security Best Practices for Protecting Your HIPAA-Compliant Data (securitymetrics.com)](https://www.securitymetrics.com/blog/5-security-best-practices-protecting-your-hipaa-compliant-data)

<https://www.revelemd.com/blog/top-10-most-common-hipaa-violations>

<https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html>

<https://www.hipaajournal.com/hipaa-resources/>

<https://www.hipaajournal.com/hipaa-compliance-checklist/>

<file:///C:/Users/Nicole/Downloads/HIPAAComplianceChecklistDownload.pdf>

[Security Content Automation Protocol | CSRC (nist.gov)](https://csrc.nist.gov/projects/security-content-automation-protocol/hipaa)