CRAIG PETERSØN

AMERICA'S LEADING SECURITY COACH

# HIPAA CYBERSECURITY CHEAT SHEET

## ① HIPAA


HIPAA compliance is a must. HIPAA guidelines protect patients' health information, ensuring that it is stored securely, and used correctly. HIPAA does several important things. It reduces health care abuse and fraud and sets security standards for electronic billing of healthcare. It also does the same for the storage of patients' healthcare information. The Act mandates the protection and handling of medical data, ensuring that healthcare data is kept private.

## ② Compliance with HIPAA


HIPAA compliance guidelines are incredibly essential. Failure to comply can put patients' health information at risk. Breaches can have a disastrous impact on a company's reputation, and you could be subject to disciplinary action and strict violation fines and penalties by CMS/OCR. Organizations that fail to implement adequate systems can suffer significant damage. The remediation and penalties are substantial If a breach takes place.

## HIPAA Privacy Rule ③


It applies to three types of companies: providers, supply chain (contractors, vendors, etc.) and now service providers (such as data centers and cloud services providers). All health plans and healthcare clearinghouses must be HIPAA compliant. These rules also apply to healthcare providers who conduct electronic health-related transactions. The Privacy Rule requires that providers put safeguards in place to protect their patients' privacy. The safeguards must shield their PHI. The HIPAA Privacy Rule also sets limits on the disclosure of ePHI.



**Continue reading on next page >**

# HIPAA CYBERSECURITY CHEAT SHEET



## ④ HIPAA Security Rule


The safeguards of the HIPAA Security Rule are broken down into three main sections. These include technical, physical, and administrative safeguards.

**Technical Safeguards:**

In the HIPAA Security Rule there are four categories in the technical safeguards.

- First is access control. These controls are designed to limit access to ePHI. Only authorized persons may access confidential information.
- Second is audit control. Covered entities must use hardware, software, and procedures to record ePHI. Audit controls also ensure that they are monitoring access and activity in all systems that use ePHI.
- Third are integrity controls. Entities must have procedures in place to make sure that ePHI is not destroyed or altered improperly. These must include electronic measures to confirm compliance.
- Lastly, there must be transmission security. Covered entities must protect ePHI whenever they transmit or receive it over an electronic network.

**Physical Safeguards:**

Requires that all covered organizations implement physical safeguards to protect ePHI. The physical safeguards cover the facilities where data is stored, and the devices used to access them. Access must be limited to authorized personnel. Workstation and device security are also essential. The removal, transfer, destruction, or re-use of such devices must be processed in a way that protects ePHI.

## HIPAA Security Rule (con't.) ④

**Administrative Safeguards:**

In the HIPAA Security Rule there are five categories in the Administrative safeguards.

- First, there must be a security management process. The covered entity must identify all potential security risks to ePHI. It must analyze them. Then, it must implement security measures to reduce the risks to an appropriate level.
- Second, there must be security personnel in place. Covered entities must have a designated security official. The official's job is to develop and implement HIPAA-related security policies and procedures.
- Third, covered entities must have an information access management system. The Privacy Rule limits the uses and disclosures of ePHI. Covered entities must put procedures in place that restrict access to ePHI to when it is appropriate based on the user's role.
- Fourth, covered entities must provide workforce training and management. They must authorize and supervise any employees who work with ePHI.



**Continue reading on next page >**

# HIPAA CYBERSECURITY CHEAT SHEET



## ④ HIPAA Security Rule (con't.)

These employees must get training in the entity's security policies. Likewise, the entity must sanction employees who violate these policies.

- Fifth, there must be an evaluation system in place. Covered entities must periodically assess their security policies and procedures.



CRAIG PETERSØN

AMERICA'S LEADING SECURITY COACH