HIPAA-Compliance Cheat Sheet

No.	Standard	Implementation Specification	Type	CFR Code	Description
TECHNICAL SAFEGUARDS					
Technical Implementations					
1	Access Control	Unique User Identification	Required	164.312(a)(1)	Assign a unique name and/or number for identifying and tracking user identity
2	Audit Controls	Audit Controls	Required	164.312(b)	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI
3	Access Control	Automatic Logoff	Addressable	164.312(a)(1)	Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity
4	Access Control	Encryption & Decryption	Addressable	164.312(a)(1)	Implement a mechanism to encrypt and decrypt ePHI
5	Integrity	Mechanism to Authenticate ePHI	Addressable	164.312(c)(1)	Implement electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner
6	Transmission Security	Integrity Controls	Addressable	164.312(e)(1)	Implement security measures to ensure that electronically transmitted ePHI is not improperly modified without detection until disposed of
7	Transmission Security	Encryption	Addressable	164.312(e)(1)	Implement a mechanism to encrypt ePHI whenever deemed appropriate
Procedural Implementations					
8	Access Control	Emergency Access Procedure	Required	164.312(a)(1)	Establish (and implement as needed) procedures for obtaining necessary ePHI during an emergency
9	Authentication	Authentication	Required	164.312(d)	Implement procedures to verify that a person or entity seeking access to ePHI is the one claimed
PHYSICAL SAFEGUARDS					
Technical Implementations					
1	Workstation Use	Workstation Use	**Required**	164.310(b)	Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access ePHI
2	Workstation Security	Workstation Security	**Required**	164.310(c)	Implement physical safeguards for all workstations that access ePHI, to restrict access to authorized users
3	Device & Media Controls	Disposal	**Required**	164.310(d)(1)	Implement policies and procedures to address the final disposition of ePHI, and/or the hardware or electronic media on which it is stored
4	Device & Media Controls	Media Re-Use	**Required**	164.310(d)(1)	Implement procedures for removal of ePHI from electronic media before the media are made available for re-use
5	Device & Media Controls	Data Backup & Storage	**Addressable**	164.310(d)(1)	Create a retrievable, exact copy of ePHI, when needed, before movement of equipment
Procedural Implementations					
1	Facility Access Controls	Contingency Operations	**Addressable**	164.310(a)(1)	Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the Disaster Recovery Plan and Emergency Mode Operations Plan in the event of an emergency
2	Facility Access Controls	Facility Security Plan	**Addressable**	164.310(a)(1)	Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft
3	Facility Access Controls	Access Controls & Validation Procedures	**Addressable**	164.310(a)(1)	Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision
4	Facility Access Controls	Maintenance Records	**Addressable**	164.310(a)(1)	Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (e.g. hardware, walls, doors, and locks)
5	Device & Media Controls	Accountability	**Addressable**	164.310(a)(1)	Maintain a record of the movements of hardware and electronic media and any person responsible

ADMINISTRATIVE SAFEGUARDS					
Technical Implementations					
No.	**Standard**	**Implementation Specification**	**Type**	**CFR Code**	**Description**
1	Security Management Process	Risk Analysis	**Required**	164.308(a)(1)	Perform and document a risk analysis to see where PHI is being used and stored in order to determine all the ways that HIPAA *could be* violated
2	Security Management Process	Risk Management	**Required**	164.308(a)(1)	Implement sufficient measures to reduce these risks to an appropriate level
3	Security Management Process	Information Systems Activity Reviews	**Required**	164.308(a)(1)	Regularly review system activity, logs, audit trails, etc.
4	Information Access Management	Multiple Organizations	**Required**	164.308(a)(4)	Ensure that PHI is not accessed by parent or partner organizations or subcontractors that are not authorized for access
Procedural Implementations					
1	Security Management Process	Sanction Policy	**Required**	164.308(a)(1)	Implement sanction policies for employees who fail to comply
2	Assigned Security Responsibility	Officers	**Required**	164.308(a)(2)	Designate HIPAA Security and Privacy Officers
3	Security Incident Procedures	Response & Reporting	**Required**	164.308(a)(6)	Identify, document, and respond to security incidents
4	Contingency Plan	Contingency Plans	**Required**	164.308(a)(7)	Ensure that there are accessible backups of ePHI and that there are procedures for restore any lost data
5	Contingency Plan	Emergency Mode	**Required**	164.308(a)(7)	Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of ePHI while operating in emergency mode
6	Evaluations	Evaluations	**Required**	164.308(a)(8)	Perform periodic evaluations to see if any changes in your business or the law require changes to your HIPAA compliance procedures
7	Business Associate Agreements	Business Associate Agreements	**Required**	164.308(b)(1)	Have special contracts with business partners who will have access to your PHI in order to ensure that they will be compliant. Choose partners that have similar agreements with any of their partners to which they are also extending access
8	Information Access Management	ePHI Access	**Addressable**	164.308(a)(4)	Implement procedures for granting access to ePHI that document access to ePHI or to services and systems that grant access to ePHI
9	Security & Awareness Training	Security Reminders	**Addressable**	164.308(a)(5)	Periodically send updates and reminders about security and privacy policies to employees
10	Security & Awareness Training	Protection Against Malware	**Addressable**	164.308(a)(5)	Have procedures for guarding against, detecting, and reporting malicious software
11	Security & Awareness Training	Login Monitoring	**Addressable**	164.308(a)(5)	Institute monitoring of logins to systems and reporting of discrepancies
12	Security & Awareness Training	Password Management	**Addressable**	164.308(a)(5)	Ensure that there are procedures for creating, changing, and protecting passwords
13	Workforce Security	Employee Oversight	**Addressable**	164.308(a)(3)	Implement procedures to authorize and supervise employees who work with PHI, and for granting and removing PHI access to employees. Ensure that an employee's access to PHI ends with termination of employment
14	Contingency Plan	Contingency Plans Updates & Analysis	**Addressable**	164.308(a)(7)	Have procedures for periodic testing and revision of contingency plans

Required = Items that MUST be implemented

Addressable = Items that must be implemented IF it is reasonable and appropriate to do so

Published by PropellerHeads, Inc.| MyPropellerHeads.com | Updated 01/2020