HIPAA Security and HITECH Compliance Checklist

A Compliance Self-Assessment Tool

AAPC
PHYSICIAN SERVICES
Compliant and Profitable Practices

HIPAA SECURITY AND HITECH CHECKLIST

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires physicians and other healthcare providers who conduct electronic transactions to adopt certain security measures to safeguard protected health information (PHI) in electronic form. The Security Rule is designed to not only safeguard confidentiality of PHI but also ensures that the data you transmit or receive are not altered in the process and that the data in your information systems are available to appropriate individuals. The Security Rule is comprised of 3 main components:

- **Administrative Safeguards**
  These safeguards address your operations. They include assigning responsibility to someone for security and having policies and procedures in place to direct your security efforts.

- **Physical Safeguards**
  These safeguards address physical and facility related matters such as locks and keys, where computers are located, how electronic media are disposed of, and generally how to make the environment safe.

- **Technical Safeguards**
  These safeguards are focused on controlling access to systems and electronic PHI. They identify who may have access to information systems, provide access to sets of data and specific functions in systems, audit persons who have used the systems, and protect the systems from malicious software.

Within each of the 3 components are a set of standards along with implementation specifications. Each Security Rule standard is a requirement that the covered entity must comply with respect to the electronic PHI it creates, transmits or maintains. In some cases, specifications have been designated as "Addressable Specifications" meaning that if the specification is not applicable to your practice, then the practice does not have to formulate policies and procedures, but do have to identify why the standard does not apply. However, most addressable specifications that are found in the Security Rule can be applied to most practices in a reasonable way.

How to Use the HIPAA Privacy Checklist

The checklist provides a detailed review of each of the compliance requirements under HIPAA Security and the HITECH Act. The check list has been designed to help practices easily understand what is required of them and evaluate if they are compliant. Each section includes:

- Review of required standards
- Implementation specifications under each standard
- Guidance and easy to understand explanations
- Assessment guidelines to ensure appropriate compliance
- Reference for applicable forms. The complete AAPC Physician Service Compliance Toolkit contains over 70 forms that are ready to use or can be customized for your specific medical practice. Forms referenced in the checklist correspond to the applicable forms provided in the Compliance Toolkit.

Administrative Safeguards HIPAA Regulation: 164.308	**Security management - 164.308** The Security Management standard is intended to establish within a practice the implementation of appropriate policies and procedures to prevent, detect, contain, and correct security violations.

Implementation Specification	Guidance	Assessment	Y / N	Risk Rating / Comments
Assign Security Responsibility 164.308(a)(2) Practices are required to identify a security official who is responsible for the development and implementation of the policies and procedures required by HIPAA Security Rule. <u>Applicable Forms:</u> Security Officer Job Description	***This is a required standard for all practices.*** Primary responsibilities of the medical practice privacy security officer should include: • Establishing a security program and overseeing its implementation and compliance with regulatory standards. • Ensure purchases of information technology are consistent with the practice's security policies. • Investigating security incidents and regularly review IT system activity to ensure compliance. • Ensure appropriate security training and awareness among practice staff. • Annual review of compliance with security requirements, policies, and standards.	The practice has designated a Privacy Security Officer and has appropriate job description and duties documented. *(This can be the same person as the HIPAA Compliance Officer).*		
Risk Analysis 164.308(a)(1)(ii)(A) Practices are required to conduct an assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI. This process is intended to identify current security risks. <u>Applicable Forms:</u> HIPAA Security / HITECH Checklist Equipment / IT Inventory Sheet	***This is a required standard for all practices.*** The risk assessment should include the following: • Identifies potential security risks to ePHI • Rates the likelihood of occurrence for security risk. • Rates the extent of damage each risk might cause. • Description of controls the practice has implemented to limit any vulnerability or reduce risk. In addition to the risk analysis, the practice should include an inventory of all IT equipment and systems used (software, hardware) and who has access to each system.	The practice has conducted and documented a risk assessment to evaluate and indentify any vulnerabilities and their impact to ePHI within the last 3 years.		
		As part of the risk assessment, the practice maintains an inventory of all information technology assets / equipment.		
		The designated security official <u>annually</u> reviews, updates and approves the risk analysis.		
Risk Management 164.308(a)(1)(ii)(B) Practices are required to implement security measures sufficient to reduce risks and vulnerabilities identified during the risk analysis and to stay compliant with HIPAA security standards. This process is intended to ensure ongoing control of security risks. <u>Applicable Forms:</u> Employee Training Attendance Sheet Employee Compliance Training Log	***This is a required standard for all practices.*** A one-time comprehensive HIPAA security training is required for all employees. Ongoing education of employees pertaining to HIPAA updates throughout the year should be provided and employers should keep employees updated of any significant policy or procedure changes. All employees should receive annual re-training of HIPAA standards	The practice regularly reviews all HIPAA Security policies and procedures and updates them as needed.		
		Employees have received training and awareness on security measures. Additionally, employees date and initial updates throughout the year and kept in file.		

Implementation Specification	Guidance	Assessment	Y / N	Risk Rating / Comments
Sanction Policy 164.308(a)(1)(ii)(C) A practice is required to apply appropriate sanctions against employees who fail to comply with the practice's security policies and procedures. Applicable Forms: Sanction Policy Template Employee Disciplinary Action Form	***This is a required standard for all practices.*** The policy should incorporate penalties that are based on and appropriate for the severity of the violation and also outline the process for reporting non-compliant employees.	The practice has a formal, documented disciplinary policy.		
		Any disciplinary action taken is documented and maintained in the employees file.		
Information System Activity Review 164.308(a)(1)(ii)(D) Practices are required to implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. Applicable Forms: IT System Activity Review Log	***This is a required standard for all practices.*** The purpose is to ensure that someone is regularly monitoring the practice's systems for any unauthorized access.	The security official periodically reviews system activity via audit logs and access reports to identify any patterns or breaches contrary to the practice's access and security policy and procedures.		
		A record is maintained of all reviews of security incidents and system activity.		
		Incidents requiring follow up related to suspicious system activity are documented along with any corrective actions.		

Administrative Safeguards HIPAA Regulation: 164.308	**Workforce Security - 164.308(a)(3)(i)** The workforce security standard is intended to establish policies and procedures to ensure that all employees have appropriate access to ePHI and to prevent those who do not/should not have access from obtaining access to ePHI. Only those staff members or workforce members who need access to particular information should be able to view and/or modify ePHI.

Implementation Specification	Guidance	Assessment	Y / N	Comments
Authorization and/or Supervision 164.308(a)(3)(ii)(A) Practices should implement procedures for the authorization and/or supervision of employees who work with ePHI or in locations where it might be accessed. Applicable Forms: Employee IT Access List Employee Confidentiality Statement	***This is not a required standard (addressable)*** Access to ePHI, should be based on the staff member's job responsibilities and qualifications. Authorization should be limited to the information the individual needs to fulfill his or her job responsibilities.	The practice has implemented procedures for the authorization or supervision of employees working with ePHI.		
		Practice has job descriptions for each job type which includes job responsibilities and what access to ePHI is appropriate for that position.		
		The administrator or security officer is responsible for reviewing access rights and determining appropriate access levels. A list is maintained documenting what systems employees have access to along with their usernames.		

Implementation Specification	Guidance	Assessment	Y / N	Comments
		Staff members not authorized to access ePHI are supervised when they have an opportunity to obtain or access such information. (e.g. maintenance personnel working on computer).		
		All employees have signed a confidentiality statement. The practice maintains a list.		
Workforce Clearance Procedures 164.308(a)(3) Implement procedures to determine that the access of a workforce member to ePHI is appropriate.	***This is not a required standard (addressable)*** The practice should evaluate potential employees to determine their character is suitable to adhere to your policies and procedures for protecting ePHI.	The practice has a formal process for screening job candidates and conducting background checks as part of the hiring process.		
Termination Procedures 164.308(a)(3) Implement procedures for terminating access to ePHI when the employment of a workforce member ends. <u>Applicable Forms:</u> Employee Termination Checklist	***This is not a required standard (addressable)*** The practice is responsible for ensuring all access privileges are no longer active when an employee or contractor leaves (voluntarily or involuntarily). This includes access to data, networks, email accounts, work station and servers, as well as any physical access or keys to access areas where ePHI may be located.	The practice has developed and utilizes a termination check list which includes terminating IT system privileges. *Audit Check: Review termed employee and verify system privileges have been revoked.*		
		A process is in place for disabling an employee's password and access privileges upon termination. This should occur immediately upon notifying the employee of termination.		
		Return of any related equipment, keys, security badges, PDAs is tracked and logged as part of the termination process.		
		A process is in place to ensure employees upon termination do not retain or remove from the clinic any information, computer files or equipment belonging to the clinic. For example escorting terminated employees out of the practice.		

Administrative Safeguards HIPAA Regulation: 164.308	**Information Access Management - 164.308(a)(4)** The information access management standard is intended to establish within practices policies and procedures for authorizing access to electronic PHI that are consistent with HIPAA security requirements. The purpose is to minimize any risk of inappropriate disclosure, destruction or altercation of ePHI.

Implementation Specification	Guidance	Assessment	Y / N	Comments
Isolating Health care Clearinghouse Function 164.308(a)(4) Requires clearinghouses that are part of larger organizations to implement policies and procedures that protect ePHI of the clearinghouse from unauthorized access by the larger organization.	This requirement is only applicable to a practice that may include clearinghouse services as part of their organization.	Electronic PHI processed by the clearinghouse is isolated from the other information that the practice processes.		
Access Authorization 164.308(a)(4) Implement policies and procedures for granting access to ePHI, for workstations, transactions, programs, processes, or other mechanisms.	***This is not a required standard (addressable)*** This can be covered under the workforce security standard for authorization and supervision.	Computers, terminals or other devices where ePHI can be accessed require user ID and password or supervision when being used.		
		IT systems are set up to automatically logout a user after a short period of inactivity and requires a password to re-enter the application.		
		IT system is configured to only allow the user access to predetermined sets or areas of information relevant to their job duties.		
Access Establishment and Modification 164.308(a)(4) Implement policy and procedures, based on access authorization policies, to establish, document, review, and modify user's rights of access to workstations, transactions, programs, or processes. Applicable Forms: IT Access Change Request	***This is not a required standard (addressable)*** This can be covered under the workforce security standard for authorization and supervision.	Changes to staff members access privileges is done using a formal written request which is reviewed and authorized by the appropriate security official.		

Administrative Safeguards HIPAA Regulation: 164.308	**Security Awareness and Training - 164.308(a)(5)(i)** Practices are required to implement a security awareness and training program for all members of its workforce, including management.

Implementation Specification	Guidance	Assessment	Y / N	Comments
Security Training and Reminders 164.308(a)(5) Implement periodic reminders of security and information safety best practices. <u>Applicable Forms:</u> Employee Compliance Training Log	***This is not a required standard (addressable)*** A practice is required to provide a formal initial training for all members of its workforce, as well as, any new employees. Periodic training is also required whenever the practice makes significant changes to any policies or procedures affecting ePHI security or if / when changes to HIPAA Security regulations occur.	The practice has a formal training program regarding HIPAA security rules.		
		All employees have received formal training to understand and meet the provisions of the Security Rule (documented training log).		
		The practice provides periodic updates and reminders to employees through memos, emails or signs in the practice.		
		A mechanism is in place to notify employees of any changes to IT systems or updates to security policy and procedures. All updates should be documented / dated.		
Protection from Malicious Software 164.308(a)(5) Implement procedures for guarding against, detecting, and reporting malicious software.	***This is not a required standard (addressable)*** Computer viruses and attacks pose a significant risk to any business or medical practice. Practices need to be vigilant regarding limiting the use of the internet and downloading software programs by its employees.	The practice has installed anti-virus / dedication software such as Symantec, Norton or McAfee on workstations and servers.		
		Anti-virus / dedication software in use is a current version.		
		A log is maintained of any virus / infection detections and successful eradication / cleaning.		
		Appropriate policies and procedures are in place limiting computer and email use that could pose risk of infection to the practice.		
Log-in Monitoring 164.308(a)(5) Implement procedures for monitoring and reporting log-in attempts and discrepancies.	***This is not a required standard (addressable)*** This can be covered under the security management standard for information system activity review. For added protection, it is recommended that the practice set up their system to lock out users after a specified failed number of attempts (if the system has the capability).	An audit log or exception report (indicating when there has been a problem logging in by a user) is generated and reviewed periodically.		
		A record is maintained documenting any investigations that may have resulted.		

Implementation Specification	Guidance	Assessment	Y / N	Comments
Password Management 164.308(a)(5)(ii)(D) Implement procedures for creating, changing, and safeguarding appropriate passwords. Applicable Forms: Employee IT Access List	***This is not a required standard (addressable)*** A portion of this standard can be covered under the workforce security standard for authorization and supervision.	Each employee with access to IT system is assigned a unique user ID and required to create a password in order to access the system.		
		A list is maintained documenting what systems employees have access to along with their usernames. This list is only accessible by appropriate individuals.		
		System requires employees to periodically change their passwords (minimum every 6 months).		
		A process is in place for immediate termination of an individual's password and access privileges.		
		Passwords are not written down by employees and are not shared with others.		
Security Incident Procedures 164.308(a)(6) Practices are required to identify and respond to suspected or known security incidents and mitigate, if possible any harmful effects, and document such incidents and their outcomes. Applicable Forms: Security Incident Report	***This is a required standard for all practices.*** A security incident is the "attempted or successful unauthorized access, use or disclosure, modification, or destruction of information or IT operating systems. Examples may include: stolen passwords, corrupted back-up tapes, virus attacks, accounts being used by another individual, failure to terminate an account of a former employee.	Procedures are in place for reporting security incidents. All staff has been trained on these procedures.		
		The practice maintains a security incidents report which includes a record of actions taken to resolve the issue and mitigate any future recurrence.		

Administrative Safeguards HIPAA Regulation: 164.308	**Contingency Planning - 164.308(a)(7)(i)** Requires practices to establish (as needed) policies and procedures for responding to an emergency or natural disaster. For example, fire, vandalism, system failure, floods and earthquakes may damage systems that contain electronic protected health information. This standard is intended to ensure a practice has the ability to recover its ePHI in the event of an emergency or disaster.

Implementation Specification	Guidance	Assessment	Y / N	Comments
Contingency Plan - 164.308(a)(7)(i) Applicable Forms: Practice Contingency Plan	A contingency plan helps to ensure business continuity during any type of emergency. The contingency plan should include details regarding: • What disasters could affect integrity of ePHI • Actions the practice will take to ensure access and integrity of ePHI as the result of an emergency / disaster. • The roles and responsibilities of staff in the event of an emergency or disaster.	The practice has a formal contingency plan which is reviewed and updated annually.		
Data Backup Plan 164.308(a)(7) Establish and (implement as needed) procedures to create and maintain retrievable, exact copies of ePHI during unexpected negative events.	***This is a required standard for all practices.*** As part of the overall contingency plan, the practice should create and maintain copies of its ePHI. Backups should typically occur each day and tangible copies should be stored off-site.	The practice has identified what information must be backed up, the method of back-up and frequency.		
		Verify backup copies are being created and stored according to the data backup plan.		
		Backup copies of data and ePHI are stored in a secure but accessible location and manner that prevents unauthorized access.		
Disaster Recovery Plan 164.308(a)(7) Establish (and implement as needed) procedures to restore any loss of data. Applicable Forms: Equipment / IT Inventory Sheet	***This is a required standard for all practices.*** As part of the overall contingency plan, the disaster recovery plan should outline what data must be restored and how it is to be restored. A cop of the recovery plan should be kept off-site along with the practice's copies of backup data.	The practice has established procedures for restoring ePHI that is inadvertently destroyed or corrupted. These procedures are documented in the practice's contingency plan.		
		The practice has established procedures for replacing critical equipment and applications as part of the disaster recovery plan.		
		The disaster recovery plan includes provisions for taking an inventory of any loss of or damage to equipment or data.		
Emergency Mode Operation Plan 164.308(a)(7) Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of ePHI while operating in emergency mode.	***This is a required standard for all practices.*** As part of the overall contingency plan, the emergency mode operations plan should include an emergency contact list including a list of individuals to be notified in an emergency. This should include a list of police, fire, building maintenance, pluming, and electrician numbers. Paper forms should be readily available in case of a	The contingency plan includes operating procedures during an emergency, including what essential information will be made available.		
		The emergency mode operations plan includes a list of individuals and contact information to be notified in case of an emergency, their roles and responsibilities, and alternate means of security during restoration.		

Implementation Specification	Guidance	Assessment	Y / N	Comments
	power outage (i.e. registration, consent forms and progress notes).	All staff has been trained on their responsibilities in the event of an emergency.		
		The practice has a back-up power source that allows for maintaining system integrity in the event of a power disruption. Red outlets should be installed to indicate those outlets provide electricity by back-up power source.		
Testing and Revision Procedures 164.308(a)(7) Practices should implement procedures for periodic testing and revision of contingency plans.	***This is not a required standard (addressable)*** Each component of the contingency plan (data backup, disaster recovery, and emergency mode operations) should be tested periodically to ensure its effectiveness and revised if needed to address any discrepancies.	The practices' contingency plan has been reviewed and tested within the last 12 months, and updated (if applicable).		
		Back up data has been tested to ensure accuracy of data and information and that it can be successfully restored / retrieved.		
		Emergency power supplies are tested on a routine basis.		
		Fire alarms and suppression equipment has been tested to confirm they function properly.		
		Staff has reviewed the contingency plan including roles and responsibilities within the last 12 months.		
Applications and Data Criticality Analysis 164.308(a)(7) If applicable, practices should assess the relative criticality of specific applications and data in support of other contingency plan components. <u>Applicable Forms:</u> Equipment / IT Inventory Sheet	***This is not a required standard (addressable)*** This list should be maintained as part of your Disaster Recovery Plan.	The practice has conducted a review of which applications, equipment and data are most critical for providing patient care.		
		Based on the review, the practice maintains a prioritized list to ensure the most critical applications or equipment is restored first. The list is updated annually.		
Evaluation Policy 164.308(a)(8) Perform periodic technical & nontechnical evaluations, to establish how well security policy and procedures meet the requirements of this subpart.	***This is a required standard for all practices.*** Practice must periodically evaluate their security plans and procedures to ensure their continued effectiveness. A technical evaluation should be conducted by IT experts or your vendor due to the complexity of computer systems.	The practice's compliance with security standards and implementation specifications has been evaluated within the last 12 months.		

Administrative Safeguards HIPAA Regulation: 164.308	**Business Associate Contracts and Other Arrangements - 164.308(b)(1)** A practice may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the practice's behalf only if the practice obtains satisfactory assurances that the business associate will appropriately safeguard the information.

Implementation Specification	Guidance	Assessment	Y / N	Comments
Written Contract or Other Arrangements 164.308(b)(4) Satisfactory assurances required by the business associate contract standard are documented in a written contract or other arrangement that allows business associates PHI access and confidential access of the practice. Applicable Forms: Business Associate Agreement Business Associate Checklist	***This is a required standard for all practices.*** Note, that a written contract is not required with respect to transmission of ePHI for the following TPO (Treatment, Payment and Operational) reasons: • By covered entity to a healthcare provider concerning the treatment of an individual. • By health plan, HMO or health insurance issuer on behalf of a group health plan to a plan sponsor. • From or to other agencies providing the services when the covered entity is a health plan that is a government program providing public benefits.	The practice has identified all individuals or entities that are business associates and required them to sign a business associate agreement.		
Business associate and other arrangements. 164.314 (i) The contract known as the business associate agreement between a practice and its business associate must contain the required information prescribed by the HIPAA Security Rules. If a covered entity is aware or suspects that a business associate is in material breach of the business associate's obligation under the contract, they must take reasonable steps to cure the breach or end the violation. This may involve: 1. Terminating the contract with the business associate, if feasible. 2. If termination is not feasible, report the problem to the Secretary.	*Business associate contracts.* The contract between a covered entity and a business associate must provide that the business associate will— (A) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the covered entity as required by this subpart; (B) Ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it; (C) Report to the covered entity any security incident of which it becomes aware; (D) Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract.	Business associate agreements contain appropriate assurances and termination provisions.		

Physical Safeguards HIPAA Regulation: 164.310	**Facility Access Controls - 164.310(a)(1)** A practice is required to implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

Implementation Specification	Guidance	Assessment	Y / N	Comments
Contingency Operations Procedures 164.310(a)(2)(i) Establish (and implement as needed) procedures that ensure facility access to support restoration of lost data in the event of an emergency.	***This is not a required standard (addressable)***	Staff responsible for implementing contingency plans can physically obtain back-up data sets.		
Facility Security Plan 164.310(a)(2)(ii) A practice should have policies and procedures to safeguard the facility and their equipment from unauthorized physical access, tampering, and theft.	***This is not a required standard (addressable)***	Records or computer equipment other than workstations are kept in locked areas or cabinets.		
		Only staff members authorized to use or maintain IT equipment or servers has access to secure areas (e.g. keys to locked areas are only issued to authorized individuals).		
		Back-up media stored off-site are stored in a manner that prevents physical access by anyone lacking proper authorization.		
		Contractors and maintenance personnel who are not members of the staff have signed a business associate agreement.		
		Contractors and maintenance personnel are given a unique user ID and password that enables the practice to monitor their access to the medical practice's IT resources. Ideally the system should be able to create a one-time access password.		
		Before a user ID is activated, the security official reviews with the contractor the practice's security policies and procedures and the provisions of the business associate agreement related to security.		
		The practice has appropriate fire suppression systems in place that are compliant with all safety and building codes.		
		The practice has appropriate security alarm or surveillance systems in place.		

Implementation Specification	Guidance	Assessment	Y / N	Comments
Access Control and Validation Procedures 164.310(a)(2)(iii) A practice should have procedures to control and validate individual access to facilities based on role or function; including visitor control, and access control for software testing and revision.	***This is not a required standard (addressable)***	All visitors to the medical practice register with the receptionist and sign a visitor log and are required to wear a visitor's badge.		
		Visitors to the medical practice are not left alone (except in public waiting areas).		
		Visitors to the medical practice are not allowed to roam unaccompanied by a staff member.		
Maintenance Records 164.310(a)(2)(iv) A practice is required to document repairs and modifications to the physical components of its facility which are related to security. <u>Applicable Forms:</u> Facility Maintenance Record	***This is not a required standard (addressable)*** Examples of applicable repairs may include (but not limited to) any repairs or modifications done to facility hardware, security systems, walls, doors and locks.	All repairs and/or modifications made to the building related to security are documented.		

Physical Safeguards HIPAA Regulation: 164.310	**Workstation Use - 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 electronic protected health information.

Implementation Specification	Guidance	Assessment	Y / N	Comments
This standard does not have corresponding implementation specifications. However, compliance with the standard itself is required.	***This is a required standard for all practices.*** The practice should have guidelines and policies in place to ensure appropriate use of workstations located throughout the practice including in private office areas.	Work stations located in common but non-public areas are not used to perform security related administrative functions (e.g. adjusting access rights).		
		Workstations are set up to restrict the functions it can perform based on the level of permissions assigned to each user.		
		Users are required to log off all workstations rather than leaving them unattended. This includes workstations in private offices.		
		All workstations and monitors are positioned so that they are visible only to the persons who use them or the practice uses privacy screens.		
		Workstation areas are kept clean and well organized. Paper or confidential material is securely kept.		

Physical Safeguards HIPAA Regulation: 164.310	**Workstation Security - 164.310(c)** Implement physical safeguards for all workstations that access ePHI, to restrict access to authorized users.

Implementation Specification	Guidance	Assessment	Y / N	Comments
This standard does not have corresponding implementation specifications. However, compliance with the standard itself is required.	***This is a required standard for all practices.***	Workstations are located in physically secure areas where it is not vulnerable to theft or unauthorized removal from the office.		

Physical Safeguards HIPAA Regulation: 164.310	**Device and Media Controls - 164.310(d)(1)** Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.

Implementation Specification	Guidance	Assessment	Y / N	Comments
Media Disposal & Disposition or Re-use 164.310(d)(2)(i), (ii) The practice has policies and procedures for removing ePHI from hardware or electronic media on which it is stored prior to disposal or re-use.	***This is a required standard for all practices.*** Electronic media may include (but not limited to) things such as PDAs, thumbnail drives, computers, disks, cell phones etc.	The practice has process for erasing or purging ePHI on equipment and other media that is either going to be re-used, recycled or disposed of.		
		The Security Officer checks all media or equipment to ensure ePHI has been properly removed prior to any re-use or disposal.		
Hardware & Media Accountability 164.310(d) (2)(iii) The practice is required to maintain records of the movements of hardware and electronic media, and any person responsible therefore. <u>Applicable Forms:</u> Equipment / IT Inventory Sheet	***This is not a required standard (addressable)***	The practice maintains an inventory of all equipment and property (e.g. fax, copiers, and computers) by location and person responsible for it.		
		Authorization forms and receipts are required for all major property or equipment transactions.		
		Any personal devices or laptop computers that are allowed to be removed from the clinic are properly managed / monitored. Authorization is required before any ePHI can be downloaded unto these devices.		
		Fax machines are located in a secure or supervised area.		

Implementation Specification	Guidance	Assessment	Y / N	Comments
Data Backup and Storage 164.310(d) (2)(iv) Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.	***This is not a required standard (addressable)*** The practice should make a copy of ePHI prior to moving any equipment such as computers that contains protected health information.	Before moving any equipment the practice creates back-up copies of ePHI, which are retained until the equipment has been moved and restarted.		

Technical Safeguards HIPAA Regulation: 164.312	**Access Controls - 164.312(a)(1)** Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights.

Implementation Specification	Guidance	Assessment	Y / N	Comments
General Specifications regarding email use.	***This is a required standard for all practices***. Sample Language: *"This e-mail, including attachments, may include confidential and/or proprietary information, and may be used only by the person or entity to which it is addressed. If the reader of this e mail is not the intended recipient or his or her authorized agent, the reader is hereby notified that any dissemination, distribution or copying of this e-mail is prohibited. If you have received this e-mail in error, please notify the sender by replying to this message and delete this e-mail immediately."*	All emails sent from the practice contain a confidentiality / privacy statement.		
		Web-based email account such as (but not limited to) yahoo and hotmail are not allowed to be used for transmitting any type of ePHI.		
		The clinic has a policy restricting or minimizing the use of personal email accounts from work.		
		The clinic restricts the use of instant messaging, particularly, regarding any transmission of ePHI.		
Unique User Identification 164.312(A)(2)(i) Assign a unique name and/or number for identifying and tracking user identity.	***This is a required standard for all practices.***	All employees of the clinic are given a unique username and password for email accounts and accessing IT systems.		
		Guest accounts for accessing IT systems do not permit access to ePHI or grant any administrative controls.		
		Sharing passwords or user accounts is strictly prohibited.		
		Passwords require the use of letters, numbers and/or symbols to ensure effective protection.		

Implementation Specification	Guidance	Assessment	Y / N	Comments
Emergency Access Procedure 164.312(a)(2)(ii) Establish (and implement as needed) procedures for obtaining necessary ePHI during an emergency.	***This is a required standard for all practices***.	The practice has the ability to access user accounts and reset passwords in the event of an emergency.		
Automatic Logoff 164.312(a)(2)(iii) Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	***This is not a required standard (addressable)***	Users are automatically logged off after a period of inactivity and required to log back into the system.		
Encryption and Decryption 164.312(a)(2)(iv) Implement an appropriate mechanism to encrypt and decrypt ePHI.	***This is not a required standard (addressable)*** Encrypting is not strictly required and may be costly for many practices. If this is not a viable option due to cost, you should document any alternative methods used to ensure confidentiality. Examples may include using password protection of documents or files containing ePHI and/or prohibiting the transmission of ePHI via email. *Fax machines do not require any special encryption.*	ePHI that is transmitted via email is encrypted.		
		PDAs or other mobile devices are not used to transmit or receive ePHI unless they have been encrypted.		

Technical Safeguards HIPAA Regulation: 164.312	**Audit Controls - 164.312(b)** Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.

Implementation Specification	Guidance	Assessment	Y / N	Comments
This standard does not have corresponding implementation specifications. However, compliance with the standard itself is required.	***This is a required standard for all practices***. Most information systems contain audit controls that allow for tracking of system use and resources. When looking for security issues, things like failed login attempts can help alert you to any possible issues.	Information systems used by the practice maintain a log of activity including user access and transmissions of ePHI (e.g. billing transactions).		
		Activity logs are periodically reviewed to identify any potential security issues.		

Technical Safeguards HIPAA Regulation: 164.312	**Integrity Controls Policy -** 164.312(c)(1) Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

Implementation Specification	Guidance	Assessment	Y / N	Comments
Mechanism to Authenticate Electronic PHI 164.312(c)(2) Implement electronic mechanisms to corroborate that ePHI not been altered or destroyed in an unauthorized manner.	***This is not a required standard (addressable)***	Only authorized individuals are able to access and alter ePHI.		

Technical Safeguards HIPAA Regulation: 164.312	**Person Or Entity Authentication - 164.312(d)** Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

Implementation Specification	Guidance	Assessment	Y / N	Comments
This standard does not have corresponding implementation specifications. However, compliance with the standard itself is required.	***This is a required standard for all practices.***	All systems used by the practice containing ePHI require the user to authenticate themselves prior to accessing the system (e.g. such as a password or PIN).		

Technical Safeguards HIPAA Regulation: 164.312	**Transmission Security - 164.312(e)(1)** Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

Implementation Specification	Guidance	Assessment	Y / N	Comments
Integrity Controls 164.312(e)(2)(i) Implement security measures to ensure that electronically transmitted ePHI is not improperly modified without detection until disposed of.	***This is not a required standard (addressable)*** This standard is focused on ensuring appropriate controls to help maintain the integrity of your records and prevent any accidental or intentional altercation or destruction of ePHI during the transmission process. Various software can be used such as: **Checksum** Adds up components of files and compares them between the old and new file to ensure nothing was corrupted. **Error detecting software** Detects and reports any errors that may occur during data transmission.	The practice has implemented mechanisms that can be used to confirm ePHI has not been altered.		

Implementation Specification	Guidance	Assessment	Y / N	Comments
Encryption 164.312(e)(2)(ii) Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	***This is not a required standard (addressable)*** Based on your required risk analysis determine if encryption is needed to protect the transmission of ePHI between your office and outside organizations. This should be addressed under Encryption and Decryption 164.312(a)(2)(iv)	NA		

Breach Notification HIPAA Regulation: 164.404	**Breach Notification** The Breach Notification rule establishes the requirements a medical practice must follow in the event of a breach (unauthorized disclosure or use) of unsecured protected health information.

Implementation Specification	Guidance	Assessment	Y / N	Comments
General Rule. Under HIPAA a breach is considered to have occurred when there is a disclosure or use of "unsecured" protected health information that poses a significant risk of financial, reputational or other harm to the affected individual. Unsecured PHI means that the information has not been rendered unusable, unreadable, or indecipherable to someone who has accessed it without authorization. <u>Applicable Forms</u>: Breach Notification Letter to HHS Breach Notification Letter to Individual Breach Notification Letter to Media HIPAA Incident & Resolution Form HIPAA Incident Summary Log Breach Notification Checklist	Breaches do not include: • Unintentional access or use of PHI by an employee or person acting under the authority of the clinic or a business associate, if access or use was made in good faith and within the scope of authority and does not result in further use or disclosure of the information. • Any inadvertent disclosure between individuals who are authorized to access PHI within the clinic or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed. • If there is a good faith belief by the clinic or business associate that the unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.	The practice has a policy and procedure in place outlining notification protocols in case of a breach related to protect health information.		
	Individual Notification Requirements Your clinic is deemed responsible beginning the first day that a breach is discovered. The practice is required to notify each individual who's PHI has been, or is reasonably believed to have been accessed or used as a result of the breach. • A practice is required to provide notification no later than 60 calendar days after discovery of a breach. • Notification should be sent first class mail to the last known address, or electronic mail (if approved by the individual). If the individual is deceased, notice should be sent to their next of kin or personal representative. • If there is urgency because of possible imminent misuse of unsecured protected health information, the covered entity may provide information to individuals	The practice maintains on file all documented incidents using an Incident and Resolution Form.		

Implementation Specification	Guidance	Assessment	Y / N	Comments
	by telephone or other means. The notification must include: • A brief description of what happened • The date of the breach and the date of discovery (if known) • Description of the types of information involved • Steps individuals should take to protect themselves • Description of what the practice involved is doing to investigate the breach, mitigate any damage and action taken to protect against any further breaches • Contact information for the practice			
	Media Notification Requirements If a breach entails more than 500 individuals, than the Media is required to be notified in the form of a press release, otherwise there is no requirement to notify the media.	The media was notified of any breaches entailing 500 or more individuals (if applicable).		
	Secretary Notification Requirements If a breach includes individuals of 500 or less, the practice must notify the Secretary of the Department of Health and Human Services through the HHS website. The report can be made annually. For breaches involving 500 or more individuals, the report must be filed within 60 days.	The practice maintains a summary log of all documented incidents. The log is used to provide the required report to HHS annually for all incidents involving less than 500 individuals.		