**HIPAA Compliance Checklist for “Covered Entity” Healthcare Providers**

**Free & Charitable Clinic HIPAA Toolbox**

**May 2014**

| **Regulatory References[[1]](#footnote-1)**  | **Description** | **Status** |
| --- | --- | --- |
| **A. POLICIES AND PROCEDURES** |
| ***Security Policies*** |
| 164.308(a)(1)(i) | **Security Management Process Policies and Procedures** – policies and procedures addressing the following:* Conducting of an assessment of potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI
* Updating risk assessment on periodic basis and when environmental and operational changes occur that may impact ePHI systems
* Sanctions against workforce members who fail to comply with security policies and procedures
* Review of information system activities (audit logs, access reports, security incident reports)
 |  |
| 164.308(a)(3) 164(a)(4)(i) | **Workforce Security and Information Access Management Policies and Procedures** – policies and procedures addressing the following:* Ensuring that members of the workforce have appropriate access to ePHI and preventing those workforce members who should not have access from obtaining access
	+ Granting access to ePHI
	+ Reviewing and modifying access to ePHI
	+ Terminating access to ePHI and recovery of access control devices when employment ends
* Access controls (passwords, etc.)
 |  |
| 164.308(a)(6)(i) | **Security Incident Policies and Procedures** – policies and procedures addressing the following:* Identifying, responding to, reporting, documenting, mitigating, and conducting post-incident analysis of security incidents
* Interplay with Breach Notification policies and procedures
 |  |
| 164.308(a)(7)(i) | **Contingency Plan Policies and Procedures** – policies and procedures addressing the following:* Identification of foreseeable emergencies compromising access to ePHI, measures taken to prevent emergencies, recovery of data in the event of emergency, and periodic testing and revision of emergency system, including specifically:
	+ Data backup – identifying critical applications, data, operations, and manual and automated processes involving ePHI to be backed up and creating and maintaining retrievable exact copies of ePHI in the event of an interruption in access
	+ Emergency mode operation plan – enabling continuation of critical business processes and protecting ePHI while operating in emergency mode, including how key personnel will access needed data and how data used in an emergency will be stored
	+ Disaster recovery plan – restoring data lost in the event of an emergency and permitting facility access in support of restoration of lost data
 |  |
| 164.310(a)(1) | **Facility Access Controls Policies and Procedures** – policies and procedures addressing the following:* Limiting physical access to electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed
* Safeguarding the facility and equipment from unauthorized physical access, tampering, and theft
* Controlling access by staff, contractors, visitors, and probationary employees
* Validating a person’s access to facilities based on role or function
* Documenting repairs and modifications to physical components of facility related to security (hardware, walls, doors, locks, etc.)
 |  |
| 164.310(b) | **Workstation Use Policies and Procedures** – policies and procedures addressing the following:* Classifications of workstations by type, use, capabilities, and allowable activities
* Proper functions of company workstations (for example, do specific workstations have dedicated uses such as patient care or billing functions?)
* Physical attributes of surroundings of specific workstations (for example, is computer in a private area, behind a locked door, etc.?)
* Preventing unauthorized access to an unattended workstation and limiting viewing of sensitive information (for example, automatic log off)
 |  |
| 164.310(d)(1) | **Device and Media Controls Policies and Procedures** – policies and procedures addressing the following:* Tracking of receipt and removal of hardware and electronic media containing ePHI into and out of the facility and movement within the facility
* Disposal of hardware, software, and ePHI data
* Protection of data in storage
* Removal of ePHI before reusing electronic media
 |  |
| 164.312(a)(1) | **Access Control Policies and Procedures** – policies and procedures addressing the following:* Allowing access to ePHI systems to only those persons that have been properly granted access
* Establishment of unique user identification number for access to ePHI
* Activity tracking and review on a periodic basis
* Granting authority to add, modify, or delete user access
* Electronic procedures that terminate an electronic session after a predetermined time of inactivity
* How access to ePHI during an emergency is appropriately limited
* Removal of user access upon termination or change in position
* Encryption standards to protect ePHI
 |  |
| 164.312(c)(1) | **Data Integrity Policies and Procedures** – policies and procedures addressing the following:* Protecting ePHI from improper alteration or destruction (for example, regulating authority to edit files or maintaining firewalls and anti-virus software)
* Authenticating data
 |  |
| HIPAA Security Guidelines on Remote Access (Released on 12/28/2006) | **Remote Access Policies and Procedures** – policies and procedures addressing the following:* + Access – who should be granted access and for what data? Risk management strategies suggested by Office for Civil Rights (“OCR”) include: a two-factor authentication for granting remote access; establishing procedures for session termination on inactive portable/remote devices; installing firewalls and updated virus protection software
	+ Storage – what are the security requirements for media and devices that contain ePHI and are moved beyond Company’s physical controls? Risk management strategies suggested by OCR include tracking devices in case of loss or theft; encrypting portable/remove devices that store ePHI, use of biometrics, developing process to ensure backup of all ePHI entered into remote systems; prohibiting downloading of ePHI onto remote systems without an operational justification
	+ Transmission – how does Company ensure the integrity and safety of ePHI sent over networks? Risk management strategies suggested by OCR include prohibiting transmissions of ePHI via open networks when possible; use of secure connections for email; implementing encryption solutions
 |  |
| ***Data Breach Notification Policies*** |
| 164.402 (Definition of Breach)164.404 -408 (Notification Requirement) | **Breach Notification Policies and Procedures** – policies and procedures addressing the following:* Preventing, identifying, and mitigating breaches of unsecured PHI
* Conducting risk assessment
* Notification of individuals and government authorities, as necessary
* Documentation
 |  |
| ***Privacy Policies***  |
| 164.502 164.504164.506 164.508164.510164.520 | **Confidentiality of PHI Policies and Procedures** – policies and procedures addressing:* Disclosures for treatment, payment, or healthcare operations purposes
* Other permissible disclosures (ensure consistency with Notice of Privacy Practices)
* Disclosures to personal representatives and individuals involved in a patient’s care
* Disclosures to Business Associates
* Determining whether authorization is required for disclosure
* Notice of Privacy Practices and procedure for distribution to patients and receipt of acknowledgment from patients

*Ensure new business associate agreements comply with the Omnibus Final Rule and update current agreements as they are renewed. Review Notice of Privacy Practices for compliance with the Omnibus Final Rule.*  |  |
| 164.508 | **Patient Authorization Policies and Procedures** – policies and procedures regarding solicitations of patient authorizations regarding uses and disclosures covering marketing (i.e., the receipt of financial remuneration from a third party in exchange for making communications to individuals), sale of PHI and any other disclosures for which authorization is required.  |  |
| 164.514 | **“Minimum necessary” Policies and Procedures** – policies and procedures limiting uses or disclosures of PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. |  |
| 164.522 | **Patient Requests for Additional Privacy Protections and Alternative Confidentiality Communications of PHI** – policies and procedures addressing:* Handling, complying with, and terminating requests from or on behalf of individuals to restrict uses and disclosures of PHIs
* Handling, complying with, and terminating requests from or on behalf of individuals for confidential communications
 |  |
| 164.524 | **Patient Requests for Access to PHI Policies and Procedures** – policies and procedures for providing and denying individuals with access to designated record sets.*(Ensure procedures comply with the Omnibus Final Rule*.) |  |
| 164.526 | **Patient Requests to Amend PHI Policies and Procedures** – policies and procedures for handling PHI amendment requests. |  |
| 164.528 | **Patient Requests for an Accounting of Disclosures** **Policies and Procedures** – policies and procedures for tracking disclosures of ePHI and providing accountings with the minimum information and within the timeframe required by the Privacy Rule. |  |
| 164.508 164.512(i)164.514 | **Uses and Disclosures for Research Purposes Policies and Procedures** (if applicable) – policies and procedures for use and disclosure of PHI for research, including policies regarding creating de-identified data sets and limited data sets. |  |
| 164.508(a)(3) 164.514(f) | **Uses and Disclosures for Fundraising and Marketing Policies and Procedures** (if applicable) – policies and procedures for the use and disclosure of PHI for fundraising or marketing purposes. |  |
| 164.530(a)(1)(ii) 164.530(d)(1) | **Privacy Complaints** –Policies and procedures allowing individuals to make privacy complaints and designating a contact person or office responsible for receiving such complaints. |  |
| 164.530(e) | **Workforce Sanctions** – Policies and procedures regarding appropriate sanctions against workforce members who fail to comply with privacy policies and procedures. |  |
| 164.530(f) | **Mitigation** – Policies and procedures regarding mitigation, to the extent practicable, of any known harmful effect of a use or disclosure of PHI in violation of policies and procedures. |  |
| 164.530(g) | **Anti-Retaliation** – Policies and procedures regarding anti-retaliation against workforce members who disclose HIPAA violations. |  |
| 164.530(i) | **Documentation** – Policies and procedures for documenting compliance matters and ensuring document retention. Policy must provide that documents must be retained for six years from the date of creation or the date last in effect, whichever is later. |  |
| **B. TECHNICAL, PHYSICAL AND ADMINISTRATIVE SAFEGUARDS[[2]](#footnote-2)** |
| 164.308(a)(1)(ii)(A) | **Risk Assessment** –Complete an accurate and thorough assessment of potential risks and vulnerabilities. These may include natural threats (e.g., floods, earthquakes, power failures, etc.), intentional threats (e.g., computer/network based attacks, malware, etc.), and unintentional threats (e.g., inadvertent data entry or other actions). |  |
| 164.308(a)(1)(ii)(D) | **Information Activity Review** – Implement procedures to regularly review records of information activity such as audit logs, access reports, and security incident tracking. Implement process for documenting and providing a report of attempts (including those that are unsuccessful) to access information systems. |  |
| 164.308(a)(2) | **Security Official** – Identify a security official who is responsible for the development and implementation of policies and procedures.  |  |
| 164.308(a)(8) | **Review and Maintenance** – Establish a plan for periodic technical and non-technical evaluation of the standards under the HIPAA Security Rule in response to environmental or operational changes affecting the security of ePHI. Implement process for documenting compliance decisions and activities. |  |
| 164.310(c) | **Physical Access Controls** – Implement physical safeguards for all workstations that access ePHI to restrict access to authorized users. |  |
| 164.312(a)(2)(i) | **User Identification** –Assign a unique name and/or number for identifying and tracking user identity. |  |
| 164.312(b) | **Audit Controls** – Implement audit controls, hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI. |  |
| 164.312(d) | **User Authentication** – Establish and implement person or entity authentication procedures to verify that a person or entity seeking access to ePHI is the one claimed |  |
| 164.312(e)(1) | **Data Protection** – Implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network. |  |
| 164.312(e)(2)(ii) | **Encryption** – Implement a mechanism to encrypt ePHI when deemed appropriate.  |  |
| **C. WORKFORCE AND TRAINING** |
| 164.308(a)(5)(i) | **Security Training** – Implement security awareness and training program for all workforce members (including management), including with respect to handling of laptops and mobile devices. |  |
| 164.306(a)(4) | **Compliance Monitoring** – Implement process for monitoring and confirming that workforce members comply with policies and procedures relating to PHI. |  |
| 164.530(a)(2)164.530(b)  | **Privacy Training** – Provide training for all workforce members (including management) with respect to policies and procedures relating to PHI and implement process for documenting provision of education and training.  |  |
| 164.530(a)(2) | **New Hire Training** –Ensure new workforce members receive training within reasonable time period after joining workforce. |  |
| 164.530(a)(1)(i) | **Privacy Official** –Designate privacy official responsible for the development and implementation of policies and procedures relating to PHI. |  |
| 164.530(a)(1)(ii) | **Complaints** – Designate individual responsible for receiving privacy complaints. |  |
| **D. SALE, MARKETING AND FUNDRAISING ACTIVITIES** |
| 164.508164.514(f) | **Marketing and Fundraising** – Review any sales of PHI, marketing or fundraising activities conducted by entity either on its own behalf or on behalf of covered entities to ensure compliance with Final Rule. |  |
| **E. STATE PRIVACY AND SECURITY LAWS** |
| N/A | **State and Local Laws** – Review policies, procedures and template agreements to ensure compliance with any more stringent requirements under applicable state laws governing privacy and security. |  |

1. Reference is to 45 C.F.R. unless otherwise indicated [↑](#footnote-ref-1)
2. (A) = Addressable; (R) = Required (?) [↑](#footnote-ref-2)