

General HIPAA Compliance Policy



Introduction

HEALTHCARE ENVIRONMENT has adopted this General HIPAA Compliance Policy in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act "ARRA") and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013). We acknowledge that full compliance with the HIPAA Final Rule is required by or before September 23, 2013.

HEALTHCARE ENVIRONMENT hereby acknowledges our duty and responsibility to protect the privacy and security of Individually Identifiable Health Information ("IIHI") generally, and Protected Health Information ("PHI") as defined in the HIPAA Regulations, under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under principles of general and professional ethics. We also acknowledge our duty and responsibility to support and facilitate the timely and unimpeded flow of health information for lawful and appropriate purposes.

Scope of Policy



This policy governs General HIPAA Compliance for **HEALTHCARE ENVIRONMENT**. All personnel of **HEALTHCARE ENVIRONMENT** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.


Assumptions



- HEALTHCARE ENVIRONMENT** hereby recognizes its status as a Business Associate under the definitions contained in the HIPAA Regulations.
- HEALTHCARE ENVIRONMENT** must comply with HIPAA and the HIPAA implementing regulations, in accordance with the requirements at 45 CFR Parts 160 and 164, as amended.
- Full compliance with HIPAA is mandatory and failure to comply can bring severe sanctions and penalties. Possible sanctions and penalties include, but are not limited to: civil monetary penalties, criminal penalties including prison sentences, and loss of revenue and reputation from negative publicity.
- Full compliance with HIPAA strengthens our ability to meet other compliance obligations, and will support and strengthen our non-HIPAA compliance requirements and efforts.
- Full compliance with HIPAA reduces the overall risk of inappropriate uses and disclosures of Protected Health Information (PHI), and reduces the risk of breaches of confidential health data.
- The requirements of the HIPAA Administrative Simplification Regulations (including the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules) implement sections 1171-1180 of the Social Security Act (the Act), sections 262 and 264 of Public Law 104-191, section 105 of 492 Public Law 110-233, sections 13400-13424 of Public Law 111-5, and section 1104 of Public Law 111-148.
- Entities subject to HIPAA Rules are also subject to other federal statutes and regulations. For example, federal programs must comply with the statutes and regulations that govern them. Pursuant to their contracts, Medicare providers must comply with the requirements of the Privacy

Act of 1974. Substance abuse treatment facilities are subject to the Substance Abuse Confidentiality provisions of the Public Health Service Act, section 543 and its regulations. And, health care providers in schools, colleges, and universities may come within the purview of the Family Educational Rights and Privacy Act.

Policy Statement

- 
- ❑ It is the Policy of **HEALTHCARE ENVIRONMENT** to become and to remain in full compliance with all the requirements of HIPAA.
 - ❑ It is the Policy of **HEALTHCARE ENVIRONMENT** to fully document all HIPAA compliance-related activities and efforts, in accordance with our Documentation Policy.
 - ❑ All HIPAA compliance-related documentation will be managed and maintained for a minimum of six years from the date of creation or last revision, whichever is later, in accordance with **HEALTHCARE ENVIRONMENT**'s Document Retention policy.

Procedures

In accordance with the amended HIPAA Final Rule (Effective Date: March 26, 2013), **HEALTHCARE ENVIRONMENT** commits to enacting, supporting, and maintaining the following procedures and activities, as a minimum, as required by HIPAA:

- 
- ❑ **Privacy Policies and Procedures** -- **HEALTHCARE ENVIRONMENT** shall develop and implement written privacy policies and procedures that are consistent with the HIPAA Rules.
 - ❑ **Privacy Personnel** -- **HEALTHCARE ENVIRONMENT** shall designate a privacy official responsible for developing and implementing its privacy policies and procedures, and a contact person or contact office responsible for receiving complaints and providing individuals with information on **HEALTHCARE ENVIRONMENT**'s privacy practices.
 - ❑ **Workforce Training and Management** -- Workforce members include employees, volunteers, trainees, and may also include other persons whose conduct is under the direct control of the **HEALTHCARE ENVIRONMENT** (whether or not they are paid by **HEALTHCARE ENVIRONMENT**). **HEALTHCARE ENVIRONMENT** shall train all workforce members on its privacy policies and procedures, as necessary and appropriate for them to carry out their various functions.
 - ❑ **Sanctions** -- **HEALTHCARE ENVIRONMENT** shall have and apply appropriate sanctions against workforce members who violate its privacy policies and procedures, and/or HIPAA's Privacy and Security Rules.
 - ❑ **Mitigation** -- **HEALTHCARE ENVIRONMENT** shall mitigate, to the extent practicable, any harmful effect it learns was caused by use or disclosure of protected health information by its workforce or its business associates in violation of its privacy policies and procedures or the Privacy Rule.
 - ❑ **Data Safeguards** -- **HEALTHCARE ENVIRONMENT** shall maintain reasonable and appropriate administrative, technical, and physical safeguards to prevent intentional or unintentional uses or disclosures of protected health information in violation of the Privacy Rule and its own policies, and to limit the incidental uses and disclosures pursuant to otherwise permitted or required uses or disclosures.
 - ❑ **Complaints** -- **HEALTHCARE ENVIRONMENT** shall establish procedures for individuals to complain about its compliance with its privacy policies and procedures and the Privacy Rule. **HEALTHCARE ENVIRONMENT** shall explain those procedures in its privacy practices notice.
- 

Retaliation and Waiver -- HEALTHCARE ENVIRONMENT shall NOT retaliate against a person for exercising rights provided by HIPAA, for assisting in an investigation by HHS or another appropriate authority, or for opposing an act or practice that the person believes in good faith violates any HIPAA standard or requirement. **HEALTHCARE ENVIRONMENT** shall not require an individual to waive any right under the Privacy Rule as a condition for obtaining treatment, payment, and enrollment or benefits eligibility.



Documentation and Record Retention -- HEALTHCARE ENVIRONMENT shall maintain, until at least six years after the later of the date of their creation or last effective date, its privacy policies and procedures, its privacy practices notices, dispositions of complaints, and other actions, activities, and designations that the Privacy Rule requires to be documented.

Compliance and Enforcement

All **HEALTHCARE ENVIRONMENT** managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **HEALTHCARE ENVIRONMENT**'s Sanction Policy.

