

Agency
Street
City, State, Zip

Explanation of HIPAA and Statement of Compliance, 2017 01 01

To be compliant with HIPAA, an agency must not only be compliant but must have a written and active policy stating compliance with HIPAA regulations. This document can be found online at www.infoweb.org/HIPAA_Compliance.dot and is updated yearly.

Statement of Compliance with HIPAA

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) states:

"A covered entity must adopt reasonable and appropriate policies and procedures to comply with the provisions of the Security Rule. A covered entity must maintain, until six years after the later of the date of their creation or last effective date, written security policies and procedures and written records of required actions, activities or assessments."

Our statement

"HousingWorks.net is fully compliant with HIPAA regulations, has all safeguards in place, and performs the regular monitoring required by HIPPA regulations. Aside from the fact that our security is tighter than most banks, we also do not store any PPI information online, so it cannot be hacked. The only protected client information that is ever shared is if a client signs and mails a housing application; in other words, only the client shares his/her protected information with anyone."



**John La Bella, President
HousingWorks.net
P.O. Box 231104
Boston, MA 02123-1104**

Table of Contents

Statement of Compliance with HIPAA	1
What is HIPAA?	3
How is HIPAA enforced?	3
What are some examples of computer programs or agency work that falls under HIPAA?	3
What are the general rules?	4
What are the penalties?	4
To be compliant, what does an organization like HousingWorks have to do?	4
Risk Analysis and Management	4
Administrative Safeguards.....	5
Physical Safeguards	5
Technical Safeguards	5
'Required' versus 'Addressable' Implementation Specifications	5
Organizational Requirements	6
Policies and Procedures and Documentation Requirements	6

What is HIPAA?

HIPAA is the Health Insurance Portability and Accountability Act of 1996 (HIPAA). This law requires the Secretary of US Dept of HHS to develop regulations protecting the privacy and security of personal information.

To fulfill this mandate, HHS published two rules: the HIPAA Privacy Rule, and the HIPAA Security Rule:

- o **The Privacy Rule** establishes national standards for the protection of everyone's private information.
- o **The Security Rule** establishes a national set of security standards for protection of everyone's private information if it is stored or transferred in electronic form. This second rule addresses both:
 - a. the technology protections themselves; and
 - b. your office practices (example: 'no talking about patients in an elevator where others can hear you).

The information that is protected is sometimes called e-PHI, "electronic protected health information" or PPI "personal protected information".

How is HIPAA enforced?

Within the USHHS, the Office for Civil Rights (OCR) is responsible for enforcing the Privacy and Security Rules with voluntary compliance activities (for example, 'more training') or civil money penalties.

What are some examples of computer programs or agency work that falls under HIPAA?

- Clearinghouses such as HMIS or HousingWorks
- Hospital or Medical Records

These are computer programs that contain databases of names, health information, dates of birth, social security numbers, etc. are all stored or shared electronically. Some electronic systems are definitely not HIPAA compliant, for instance, email – you should never send a client name and social security number over email because the emails are easily and routinely 'hacked' by evil doers.

What are the general rules?

To be considered compliant, agencies must:

1. Ensure the ***confidentiality, integrity, and availability of all e-PHI** they create, receive, maintain or transmit;
2. Identify and protect against reasonably anticipated threats to the security or integrity of the information;
3. Protect against reasonably anticipated, impermissible uses or disclosures; and
4. Ensure compliance by their workforce.

***Definitions:**

- A. **Confidentiality:** means that e-PHI is not shared with unauthorized persons.
- B. **Integrity:** means that e-PHI is not altered or destroyed in an unauthorized manner – no one can delete or falsify a client's information, including your own staff.
- C. **Availability of all e-PHI:** means that e-PHI is accessible and usable on demand by an authorized person.

What are the penalties?

These penalties show how serious the Government takes HIPPA enforcement.

"The penalty may not exceed \$25,000 per year for multiple violations of the identical Privacy Rule requirement in a calendar year. HHS may not impose a civil money penalty under specific circumstances, such as when a violation is due to reasonable cause and did not involve willful neglect and the covered entity corrected the violation within 30 days of when it knew or should have known of the violation."

To be compliant, what does an organization like HousingWorks have to do?

Agencies must put safeguards in place and monitor them at specific intervals.

Risk Analysis and Management

- The Administrative Safeguards provisions in the Security Rule require covered entities to perform risk analysis as part of their security management processes. The risk analysis and management provisions of the Security Rule are addressed separately here because, by helping to determine which security measures are reasonable and appropriate for a particular covered entity, risk analysis affects the implementation of all of the safeguards contained in the Security Rule.
- A risk analysis process includes, but is not limited to, the following activities:
 - o Evaluate the likelihood and impact of potential risks to e-PHI;
 - o Implement appropriate security measures to address the risks identified in the risk analysis;
 - o Document the chosen security measures and, where required, the rationale for adopting those measures; and
 - o Maintain continuous, reasonable, and appropriate security protections.

"Risk analysis should be an ongoing process, in which a covered entity regularly reviews its records to track access to e-PHI and detect security incidents, periodically evaluates the effectiveness of security measures put in place, and regularly reevaluates potential risks to e-PHI."

Administrative Safeguards

- **Security Management Process.** As explained in the previous section, a covered entity must identify and analyze potential risks to e-PHI, and it must implement security measures that reduce risks and vulnerabilities to a reasonable and appropriate level.
- **Security Personnel.** A covered entity must designate a security official who is responsible for developing and implementing its security policies and procedures.
- **Information Access Management.** Consistent with the Privacy Rule standard limiting uses and disclosures of PHI to the "minimum necessary," the Security Rule requires a covered entity to implement policies and procedures for authorizing access to e-PHI only when such access is appropriate based on the user or recipient's role (role-based access).
- **Workforce Training and Management.** A covered entity must provide for appropriate authorization and supervision of workforce members who work with e-PHI. A covered entity must train all workforce members regarding its security policies and procedures, and must have and apply appropriate sanctions against workforce members who violate its policies and procedures.
- **Evaluation.** A covered entity must perform a periodic assessment of how well its security policies and procedures meet the requirements of the Security Rule.

Physical Safeguards

- **Facility Access and Control.** A covered entity must limit physical access to its facilities while ensuring that authorized access is allowed.
- **Workstation and Device Security.** A covered entity must implement policies and procedures to specify proper use of and access to workstations and electronic media. A covered entity also must have in place policies and procedures regarding the transfer, removal, disposal, and re-use of electronic media, to ensure appropriate protection of electronic protected health information (e-PHI).

Technical Safeguards

- **Access Control.** A covered entity must implement technical policies and procedures that allow only authorized persons to access electronic protected health information (e-PHI).
- **Audit Controls.** A covered entity must implement hardware, software, and/or procedural mechanisms to record and examine access and other activity in information systems that contain or use e-PHI.
- **Integrity Controls.** A covered entity must implement policies and procedures to ensure that e-PHI is not improperly altered or destroyed. Electronic measures must be put in place to confirm that e-PHI has not been improperly altered or destroyed.
- **Transmission Security.** A covered entity must implement technical security measures that guard against unauthorized access to e-PHI that is being transmitted over an electronic network.

'Required' versus 'Addressable' Implementation Specifications

- Covered entities are required to comply with every Security Rule "Standard." However, the Security Rule categorizes certain implementation specifications within those standards as "addressable," while others are "required." The "required" implementation specifications must be implemented. The "addressable" designation does not mean that an implementation specification is optional. However, it permits covered entities to determine whether the addressable implementation

specification is reasonable and appropriate for that covered entity. If it is not, the Security Rule allows the covered entity to adopt an alternative measure that achieves the purpose of the standard, if the alternative measure is reasonable and appropriate.

Organizational Requirements

- Covered Entity Responsibilities. If a covered entity knows of an activity or practice of the business associate that constitutes a material breach or violation of the business associate's obligation, the covered entity must take reasonable steps to cure the breach or end the violation. Violations include the failure to implement safeguards that reasonably and appropriately protect e-PHI.
- Business Associate Contracts. HHS developed regulations relating to business associate obligations and business associate contracts under the HITECH Act of 2009.

Policies and Procedures and Documentation Requirements

- A covered entity must adopt reasonable and appropriate policies and procedures to comply with the provisions of the Security Rule. A covered entity must maintain, until six years after the later of the date of their creation or last effective date, written security policies and procedures and written records of required actions, activities or assessments.
- Updates. A covered entity must periodically review and update its documentation in response to environmental or organizational changes that affect the security of electronic protected health information (e-PHI).

For more information, contact

John La Bella
HousingWorks.net
P.O. Box 231104
Boston, MA 02123-1104
support@Housingworks.net
617-504-0577 tel
617-536-8561 fax