



HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)

FREQUENTLY ASKED QUESTIONS

The Health Insurance Portability and Accountability Act (HIPAA) was signed into law in August 1996 and is designed to improve the effectiveness and efficiency of the U.S. healthcare system and mandates national standards in several areas.

Among HIPAA regulations are two important provisions:

Title I COBRA (portability) – designed to protect workers and families from the loss of health insurance coverage as the result of a job change or termination.

Title II Administrative Simplification (AS) – designed to simplify the administration of healthcare and to protect the privacy of individually identifiable health information.

The information below only covers issues related to Title II and its impact on Hygeia and our clients.

In response to the regulations issued by the U.S. Department of Health and Human Services regarding HIPAA Administrative Simplification (AS), Hygeia contracted with HIPAA consultant, Incepture, to perform an independent analysis of our operations and HIPAA-AS Gap Assessment. We reviewed all applicable business practices, and implemented policies and procedures to ensure full compliance with the standards for privacy of individual health information and electronic data interchange. In further support of our commitment to compliance, Incepture conducted a HIPAA Privacy and Security Orientation for all Hygeia staff members in Miami, Florida and Toronto, Canada.

Below are general HIPAA questions that you may find useful. For additional details on HIPAA, please visit www.hhs.gov/ocr/hipaa

1. Who must comply with HIPAA?

HIPAA regulations apply to two groups - Covered Entities and their Business Associates.

There are three (3) types of Covered Entities:

- Health Plans
- Healthcare Providers (who transmit any health information or conduct electronic health transactions)
- Healthcare Clearinghouses (that facilitate electronic transactions between health plans and providers)

Covered entities must ensure that Business Associates protect patient privacy and therefore each covered entity is required to enter into a formal "business associate agreement" before sharing Protected Health Information (PHI) with a Business Associate. This "agreement" extends accountability for protection of PHI.

HYGEIA

HEALTHCARE LEADERSHIP, ACCOUNTABILITY AND PROFIT



2. What is a Business Associate?

A Business Associate performs services for (or acts on behalf of) a covered entity. Hygeia is a Business Associate of our U.S. healthcare payer clients that are covered entities i.e. health plans and healthcare providers. As a Business Associate to these parties, Hygeia's services involve the use or disclosure of PHI and therefore Hygeia is accountable for the protection of this PHI.

Hygeia also contracts with entities that provide assistance services to travel, healthcare, financial and corporate clients. These entities would be considered Business Associates of their clients. Hygeia would be considered a Subcontractor of these Business Associates.

Our Business Associate status to our healthcare payer clients required us to execute addendums to our Network Access agreements to ensure full HIPAA compliance by those with whom we conduct business. In June 2003, Hygeia distributed these addendums to all payer-clients and has retained these signed agreements on file.

3. What is "PHI?"

Protected Health Information (PHI) includes any information relating to an individual's health or which can be used to identify the individual. PHI is not limited to written medical files, i.e. the term covers electronic transmissions, verbal communication, billing records, information written on notice boards or conference room boards etc. HIPAA requires that this information is kept secure, accurate and only available to authorized persons and for authorized uses. Examples of PHI include but are not limited to:

- Patient name; birth date, age
- Patient street addresses; city; county; precinct; zip code; telephone number; fax number; email addresses;
- Patient social security numbers; medical record numbers; health plan beneficiary numbers; account and identification numbers and any other unique identifying number or code (Hygeia ID)
- Patient claim ID; admission date, discharge date; dates of service; date of death; biometric identifiers including finger and voice prints, photographic images and any other unique identifying characteristic
- Provider Name
- Payer/Client Name

4. What Is the Privacy Rule?

The Privacy Rule is designed to maintain strong protections for the privacy of individually identifiable health information. Under the Privacy Rule, health plans, health care clearinghouses, and certain health care providers must guard against misuse of individuals' identifiable health information and limit the sharing of such information. Consumers are afforded significant new rights to enable them to understand and control how their health information is used and disclosed. The compliance deadline is April 14, 2003.

5. What is the Security Rule?

This rule specifies a series of administrative, technical, and physical security procedures for health plans, health care clearinghouses, and health care providers to use to assure the confidentiality, integrity and availability of electronic protected health information. HIPAA mandated security standards are designed to protect an individual's health information while permitting the appropriate access and use of that information

H Y G E I A

HEALTHCARE LEADERSHIP, ACCOUNTABILITY AND PROFIT



by healthcare providers, clearinghouses and health plans. The compliance deadline is April 20, 2005.

6. How does HIPAA apply to electronic transmission of patient claims?

HIPAA requires standardization in the electronic transmission of claims, administrative and financial transactions, and security for the electronic storage and transmission of patient information. This rule mandates the use of ANSI X12 format and standard coding schemes such as CPT-4 and ICD-9-CM.

Electronic transmissions would include transactions using all media, even when the information is physically moved from one location to another using magnetic tape, disk, or compact disc (cd) media. Transmissions over the Internet (wide-open), Extranet (using Internet technology to link a business with information only accessible to collaborating parties), leased lines, dial-up lines, and private networks are all included. Electronic PHI does not include paper-to-paper faxes, video teleconferencing or messages left on voicemail, because the information exchanged did not exist in electronic form before transmission.

The proposed security standard does not require the use of an electronic signature, but specifies the standard for an electronic signature that must be followed if such a signature is used. If an entity elects to use an electronic signature, it must comply with the electronic signature standard.

7. Does the HIPAA Security Rule allow for sending electronic PHI in an email or over the Internet? If so, what protections must be applied?

The HIPAA Security Rule does not expressly prohibit the use of email for sending electronic protected health information (PHI). However, the standards for access control, integrity, and transmission security require covered entities and business associates to implement policies and procedures to restrict access to, protect the integrity of, and guard against the unauthorized access to electronic PHI. This means that the covered entity and business associate must assess its use of open networks, identify the available and appropriate means to protect electronic PHI as it is transmitted, select a solution, and document the decision. The Security Rule allows for electronic PHI to be sent over an electronic open network as long as it is adequately protected.

8. Do Hygeia's electronic transmissions comply with HIPAA regulations?

All Hygeia's information transport facilities (i.e. EDI, web-browser, email fax, mail) meet the HIPAA-AS compliance guidelines.

Specific to EDI transactions, Hygeia is able to send and receive web-based electronic claim transmissions that meet HIPAA requirements. Our proprietary connection software provides a HIPAA compliant link that is in accordance with the requirements applicable to Business Associates. It is important to note that, due to the Business Associate relationship that exists between Hygeia and its international payer-clients, the HIPAA X.12 data standard is not required for claims to be sent to Hygeia.

However, we are developing a HIPAA compliant link that transforms non-standard incoming data into the X.12 format. This will allow clients to continue to communicate in a non-standard format through Hygeia's secure communication application, without the extra administrative or time expense required for HIPAA compliance, and both incoming data to Hygeia and data returned by Hygeia will be fully HIPAA compliant.



Hygeia uses an email information transport facility, which is HIPAA compliant when PHI is shared with authorized parties.

Due to HIPAA's security requirements, effective April 21, 2005, Hygeia will only send encrypted email. For clients who have entered into a security agreement with Hygeia, and have exchanged encryption keys with us, we will send email containing protected health information by encrypting the emails before transmission. For more details on encrypted email, please contact a Hygeia Client Services representative.

For clients who do not have encrypted email capabilities, Hygeia documentation that was previously sent via email will be faxed or posted on the Partners Portal. You will receive an email notification with a link directing you to retrieve the documents from the Portal.

9. Will Hygeia support clients that are not HIPAA compliant?

It is our expectation that all U.S. clients and vendors that are covered entities will become fully compliant as soon as possible, and we will work with those that are not on a case-by-case basis to minimize disruption of business operations.

10. As an international payer, does HIPAA apply to me?

In order to communicate with a Provider (Covered Entity under HIPAA law), an international payer will be impacted by the Provider's required application of HIPAA Security and Privacy standards related to the use and disclosure of "Protected Health Information" (PHI) regardless of the citizenship or residency of the patient. Therefore, a Provider may elect to not transmit PHI to any third party that is not HIPAA compliant, as knowingly transmitting this information creates a HIPAA violation exposure for the Provider.

Therefore, Hygeia recommends that international payers work through HIPAA compliant vendors for the U.S. medical cost containment needs. Due to our HIPAA compliance, Hygeia's international and domestic payers can be confident that all business processed through our organization, and communication with Providers are HIPAA compliant.

Additionally, if an international payer utilizes U.S. based subsidiaries or affiliates, or has a parent company that is U.S. based, these entities are directly subject to HIPAA requirements and regulations, which will impact all their business relationships.

Hygeia is confident that the integration of HIPAA required procedures and protocols will not impact the high service levels our clients expect from us, and will further minimize our clients' business risk.