

## HIPAA Whitepaper

### Introduction

Today, health plans, hospitals, pharmacies, doctors and other health care entities use a wide array of systems to process and track health care bills and other information. Each time a patient encounters a healthcare provider, a record of their confidential health information is made.

Congress enacted the Health Insurance Portability and Accountability Act in August 1996 to protect patient privacy. The law included provisions designed to save money for healthcare business by encouraging electronic transactions. It also required new safeguards to protect the security and confidentiality of electronic information. HIPAA included a wide array of provisions designed to make health insurance more affordable and accessible.

With support from health plans, hospitals and other health care businesses, Congress included provisions in HIPAA to require the Department of Health and Human Services (HHS) to adopt national standards for certain electronic health care transactions, codes, identifiers and security. HIPAA also set a three-year deadline for Congress to enact comprehensive privacy legislation to protect medical records and other personal health information. When Congress did not enact such legislation by August 1999, HIPAA required HHS to issue health privacy regulations.

Security and privacy standards can promote higher quality care by assuring consumers that their personal health information will be protected from inappropriate uses and disclosures. In addition, uniform national standards will save billions of dollars each year for health care businesses by lowering the costs of developing and maintaining software and reducing the time and expense needed to handle health care transactions.

### What are we protecting?

The safeguarding and handling of protected health information is the bottom line for the HIPAA rules and regulations. Protected health information is defined as any information, whether oral or recorded in any form or medium, that:

- Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and
- Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.
- Identifies the individual directly or from which the individual's identity might be derived.

### Final Rules

#### Transactions and Code Sets (45 CFR 160 and 162), "The Transaction Rule"

This rule adopts standards for electronic transactions and for code sets to be used in those transactions. It also contains requirements concerning the use of these standards by health plans, health care clearinghouses and certain health care providers.

The use of these standard transactions and code sets will improve Federal and private health programs by simplifying the administration of the system and enabling the efficient electronic transmission of certain health information. It implements some of the requirements of the Administrative Simplification subtitle of HIPAA.

**Standards for Privacy of Individually Identifiable Health Information (45 CFR 160 - 162), “The Privacy Rule”**

This rule includes standards to protect the privacy of individually identifiable health information. The rules, which apply to health plans, health care clearinghouses, and certain health care providers, present standards with respect to the rights of individuals who are the subjects of this information, procedures for the exercise of those rights, and the authorized and required uses and disclosures of this information.

The use of these standards will improve the efficiency and effectiveness of public and private health programs and health care services by providing enhanced protections for individually identifiable health information. These protections will begin to address growing public concerns that advances in electronic technology and evolution in the health care industry are resulting, or may result, in a substantial erosion of the privacy surrounding individually identifiable health information maintained by health care providers, health plans and their administrative contractors. This rule implements the privacy requirements of the Administrative Simplification subtitle of HIPAA.

**Security and Electronic Signature Standards (45 CFR 142), “The Security Rule”**

This final rule adopts standards for the security of electronic protected health information to be implemented by health plans, health care clearinghouses and certain health care providers. The use of the security standards will improve the Medicare and Medicaid programs, and other Federal health programs and private health programs, and the effectiveness and efficiency of the health care industry in general by establishing a level of protection for certain electronic health information.

**National Standard Employer Identifier (45 CFR 142), “The Security Rule”**

This rule adopts a standard for a national employer identifier and requirements concerning its use by health plans, health care clearinghouses and health care providers. The health plans, health care clearinghouses, and health care providers must use the identifier, among other uses, in connection with certain electronic transactions. The use of this identifier improves Federal and private health programs by simplifying the administration of the system and enabling the efficient electronic transmission of certain health information. It implements some of the requirements of the Administrative Simplification subtitle of HIPAA.

A unique identifying number for each employer makes it easier to determine the employer of a participant, transmit enrollment data, coordinate benefit information and track premium payments or employer contributions. In all cases where information about the employer is transmitted electronically, it identifies the employer using a standard identifier.

## **Proposed Rules**

### **National Standard Health Care Provider Identifier (45 CFR 142)**

This rule proposes a standard for a national health care provider identifier and requirements concerning its use by health plans, health care clearinghouses and health care providers. The health plans, clearinghouses and providers would use the identifier, in connection with certain electronic transactions. The use of this identifier would improve Federal and private health programs by simplifying the administration of the system and enabling the efficient electronic transmission of certain health information. It would implement some of the requirements of the Administrative Simplification subtitle of HIPAA.

Currently, health care providers are assigned non-standardized identification numbers by each of the Federal and private health plans from which they receive payments. This lack of uniformity results in a single health care provider having different numbers for each program and often multiple billing numbers issued within the same program, significantly complicating the claims submission process. Multiple numbers for providers also opens the system up to fraud, with duplicate claims filed under different provider numbers. Having a single identifier for each provider would make the exchange of data easier, reduce the complexities of reimbursement, and would enhance the ability to eliminate fraud and abuse in health care programs. A health care provider's identifier would not change with moves or changes in specialty. A provider would receive only one identifier and would not be able to receive duplicate payments from a program by submitting claims under multiple provider identifiers.

### **Who must adhere to HIPAA?**

Anyone involved in furnishing medical services or supplies must comply with HIPAA and is defined as a "covered entity." All health plans, whether private or government, must abide by HIPAA. Any business that falls under the definition of "health care clearinghouse" must conform to HIPAA. The law defines a "clearinghouse" as a public or private entity that processes, or facilitates the processing of, nonstandard data elements of health information into standard data elements.

By law, the Privacy Rule applies only to health plans, health care clearinghouses and health care providers who conduct certain financial and administrative transactions electronically. Most health care providers and health plans, however, rely upon a variety of contractors and other businesses to help them. To protect health information when it leaves the hands of those covered by the plan, the law included rules to govern "business associates."

### **What is a Business Associate?**

A business associate is a person or business that provides services for health plans, providers and clearinghouses involving the use and/or disclosure of protected health information. The business associate requirements do not apply to covered entities that disclose protected health information to providers for treatment purposes - for example, information exchanges between a hospital and physicians with admitting privileges at the hospital.

In allowing providers and plans to give protected health information to these "business associates," the Privacy Rule places the burden of complying with HIPAA on the provider or

plan. The business associate must give satisfactory assurances to the covered entity that it will:

- Use the information only for the purposes for which they were engaged by the covered entity,
- Safeguard the information from misuse,
- Help the covered entity comply with its duties to provide individuals with access to health information about them and a history of certain disclosures (e.g., if the business associate maintains the only copy of information, it must promise to cooperate and provide individuals access to information upon request).

What are a Business Associate's obligations? A Business Associate must provide to its clients (the covered entities) satisfactory assurances that it will protect information and help the client comply with its obligations under the rule. These assurances are generally provided within a written contract.

## **PhDx Systems – Your HIPAA Business Associate**

As a Business Associate and an application service provider, PhDx Systems provides web-based solutions that will keep your existing HIPAA compliance intact.

### **Concerning the Transaction Rule**

- PhDx applications can accept external data in many different formats, including XML interfaces and ASCII file import/exports.
- PhDx external interfaces can easily accommodate the specifications of the Transaction Rule if a client requires such functionality.

### **Concerning the Privacy Rule**

- PhDx client contracts specifically address points and provisions of 45 CFR 164.502(e)(2).
- PhDx employee access to protected health information is on a need-to-know basis.
- PhDx employees are all bound by confidentiality agreements to protect patient health information.
- PhDx applications can prevent the entry of any patient data until a signed patient authorization form has been received.
- PhDx reports any unauthorized release of protected health information.
- PhDx software applications are protected with role-based security for user validation, setting restrictions on application functionality and limiting data access.
- PhDx de-identifies protected health information prior to placing it in the data warehouse.

### **Concerning the Security Rule**

- PhDx client sites are accessed via 40-bit or 128-bit SSL encrypted links.
- PhDx databases are backed up daily using triply redundant methods.
- PhDx disaster recovery plans include redundant servers and offsite data backups
- PhDx Internet access is controlled and protected using firewall technology.
- PhDx intranet access is restricted to authenticated users only.
- PhDx computing facilities are protected with secure, controlled access.

## Concerning Proposed Rules and Rule Changes

- PhDx applications can easily accommodate national standard identifiers for physicians, employers and health plans.
- PhDx constantly monitors proposed changes and additions to HIPAA legislation.

## For Further Information on HIPAA

- Department of Health and Human Services, Administrative Simplification  
<http://aspe.os.dhhs.gov/admnsimp>
- Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, Title II Subtitle F Sections 261-264 and 1171-1179, titled "Administrative Simplification"  
<http://aspe.os.dhhs.gov/admnsimp/pl104191.htm>
- Transactions and Code Sets (45 CFR 160 and 162), aka "The Transaction Rule"  
<http://aspe.hhs.gov/admnsimp/final/txfin00.htm>
- Standards for Privacy of Individually Identifiable Health Information (45 CFR 160 – 164), aka "The Privacy Rule"  
<http://aspe.os.dhhs.gov/admnsimp/final/PvcPre01.htm>
- Guidance on Standards for Privacy of Individually Identifiable Health Information,  
<http://aspe.os.dhhs.gov/admnsimp/final/pvcguide1.htm>
- Security and Electronic Signature Standards (45 CFR 142), aka "The Security Rule"  
<http://aspe.os.dhhs.gov/admnsimp/nprm/seclist.htm>
- National Standard Health Care Provider Identifier (45 CFR 142)  
<http://aspe.os.dhhs.gov/admnsimp/nprm/npinprm.txt>
- National Standard Employer Identifier (45 CFR 142)  
<http://aspe.os.dhhs.gov/admnsimp/nprm/empnprm.txt>
- CFR Parts 160 and 164, Standards for Privacy of Individually Identifiable Health Information; Proposed Rule  
<http://www.hhs.gov/ocr/hipaa/propmods.txt>