# HIPAA Information

## *The Health Insurance Portability & Accountability Act*

## Overview information

In 1996, Congress passed The Health Insurance Portability & Accountability Act (HIPAA). The central objectives of the Act were to combat waste, fraud, and abuse in health care delivery and in health insurance, to improve portability and continuity of health insurance coverage in the group and individual markets, and to simplify the administration of health insurance.

The Act outlined two principle strategies to achieve these objectives:

1. Ensure the security of health care data and the absolute privacy of patient information.
2. Implement standards for the electronic exchange of healthcare information between healthcare providers, suppliers, insurers, and other entities that handle health care records.

The content and implications of these two strategies will be discussed below.

## Strategy 1: data security and privacy

Congress required the adoption of national standards to safeguard the confidentiality, integrity, and availability of electronic protected health information. The Act required the Secretary of Health and Human Services to adopt security standards that take into account the value of audit trails in computerized record systems, the technical capabilities of record systems used to maintain health information, the costs of security measures, and the need to train persons who have access to health information.

The final rule adopting HIPAA standards specifies a series of administrative, technical, and physical security procedures to assure the confidentiality of electronic protected health information. This final rule was published in the Federal Register on February 20, 2003; the compliance date is April 21, 2005. Click **here** to view a 49 page .pdf transcript.

# Strategy 1: data security and privacy, *continued …*

## *IT management implications flowing from Strategy 1*

Enterprises under HIPAA jurisdiction must conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the entity. The scope of information within this requirement includes any health care data which is created, received, maintained or transmitted by the enterprise.

Information system security is a very complex subject. A competent risk analysis would identify the vulnerabilities inherent in the collaboration between hardware, software, communication networks, and system users. Click **here** to read an article entitled "How to ensure security compliance with HIPAA" by Marcia Wilson; a key recommendation on page two of the article is quoted below:

> ***"Have an independent risk assessment performed that will allow you to establish a baseline for your company's general security posture, and work from there."***

Marcia Wilson's article states that the final rule requires the maintenance of reasonable and appropriate safeguards in three areas: administrative, physical and technical. Page 48 of the Federal Register publication presents a Security Standards Matrix that prescribes safeguards within these three areas:

**Administrative Safeguards:** *Risk analysis, risk management, information system activity review, assigned security responsibility, information access management, access authorization, protection from malicious software, log-in monitoring, password management, security incident procedures for response and reporting, data backup and disaster recovery plan*

**Physical Safeguards:** *Facility access controls, workstation use, workstation security, media re-use and disposal*

**Technical Safeguards:** *Unique user identification, automatic logoff, encryption and decryption, audit controls, person or entity authentication, transmission security, mechanism to authenticate electronic protected health information*

Here are three key definitions provided by the final rule:

"**Vulnerability**" *is a flaw or weakness in system security procedures, design, implementation, or internal controls that can be exploited by a threat and result in misuse or abuse of data. Enterprises can identify system vulnerabilities by performing a risk analysis.*

"**Risk**" *is the likelihood that a specific threat will exploit a certain vulnerability, and the resulting impact of that event.*

"**Risk analysis**" *is a systematic and analytical approach that identifies and assesses risks and provides recommendations to reduce risk to a reasonable and appropriate level. This process enables senior management to allocate appropriate resources to reduce identified vulnerabilities.*

## Strategy 2: electronic transactions & code set standards

The HIPAA rules set standards for the form/content/coding of data interchanges that are intended to enhance the operational effectiveness and efficiency of the healthcare industry. The standardized transactions employ electronic data interchange (EDI) protocols to perform health care data transfers, including XML transactions over the internet between business partners that operate in diverse software and hardware environments.

The data interchanges included within this scope are financial and administrative transactions such as health claims/attachments, eligibility for/enrollment in a health plan, health care remittances, health plan premium payments, injury reports, and health claim status.

The term 'code set' is defined by the rules to be any set of codes used for encoding data elements, such as tables of terms, medical concepts, medical diagnostic codes, or medical procedure codes.

The final rule adopting changes to the HIPAA Electronic Transactions and Code Set Standards was published in the Federal Register on February 20, 2003. Click **here** to view the 19 page .pdf transcript.

### *IT management implications flowing from Strategy 2*

Health care organizations under HIPAA jurisdiction are now trying to re-architect their software and provide web-based front ends for legacy systems and proprietary applications.

## How Unbeaten Path can help

Three of our software products hit the bulls-eye on HIPAA compliance. The two listed under Strategy 1 below are specific to the iSeries platform. The **NoSeams** product listed under Strategy 2 would be pertinent for any hardware platform.

### *Strategy 1: data security and privacy*

- ☑ **Bill of Health**™ provides 50 robust assessment reports describing your iSeries security status together with a competent prescription to address each identified vulnerability.
- ☑ **Stitch-in-Time® Data Integrity Software** observes and saves information about irregular data modification activities. It tells your security officer: 1) WHO did it, 2) exactly WHAT they did, 3) precisely WHEN they did it, and 4) HOW they did it. It even catches someone smart enough to think that they can defeat audit strategies.

### *Strategy 2: electronic transactions & code set standards*

- ☑ ***NoSeams***™ ***wwwconnections*** **for HIPAA** has an X.12 translation service that enables health care organizations to deliver HIPAA-compliant e-transactions without re-engineering their existing systems.

# More details about HIPAA

- Click **here** to view the full text of the law as passed by the congress dated August 21, 1996.
- For more information on HIPAA's privacy provisions, click **here** to access content from the Office for Civil Rights.
- For more information on HIPAA's Identifier Standards, Transactions and Code Set Standards, and Security Standards, click **here** to access the CMS web site.
- The final rule adopting the HIPAA standard unique health identifier for health care providers was published in the Federal Register on January 23, 2004. It is called the "National Provider Identifier" or the NPI. Click **here** to view the a 37 page .pdf transcript.

  *Health care providers can begin applying for NPIs on the effective date of the final rule, which is May 23, 2005. Health care providers who are under HIPAA jurisdiction must obtain and use NPIs by the May 23, 2007 compliance date. Small health care plans have until 2008 to comply.*



**Return to the IT Security Assurance page**