www.globalnts.com

About Global*Network* Technology Services

Global*Network* Technology Services provides business-focused consulting solutions to enterprise and service provider customers worldwide. Drawing upon combined strengths in technical expertise, advanced tool sets, and a proven methodology, Global*Network* Technology Services offers a high level of support through a complete portfolio of solutions focused on Infrastructure Delivery, Transaction Management, Assessment Services, and Security.

Global*Network* Technology Services is committed to delivering total client value, addressing our clients' critical business needs and the complexity and interdependence inherent in today's IT infrastructure lifecycle.

GNTS Powered Services℠

GNTS Powered Services℠ include intellectual property, tools, and a proven methodology that enable the GNTS direct delivery organization and channel partners to deliver consistent, cost-effective services on a global basis.

No. 901 1/01

U.S. Corporate Headquarters
Town Center II
1330 Lake Robbins Drive, Suite 460
The Woodlands, TX 77380
877-612-GNTS
877-612-4687

U.S. Operations Headquarters
25 Piscataqua Drive
Newington, NH 03801
877-612-GNTS
877-612-4687

Europe/Middle East/Africa
Network House
Newbury Business Park
London Road, Newbury
Berkshire, England RG14 2PZ
44-0870-200-4687

Asia Pacific
Beacon Business Park
Unit 12, 14a Rodborough Road
Frenchs Forest, Sydney NSW 2086
Australia
+612 9975 0000

Latin America
2665 South Bayshore Drive,
Suite 503
Miami, FL 33133
305-860-5337

WHITE PAPER

GlobalNetwork Technology Services

HIPAA:THE NEXT Y2K

This white paper explains HIPAA (Health Insurance Portability and Accountability Act), provides an overview of who needs to be in compliance and when, discusses compliance challenges, and offers practical guidelines for developing and executing a HIPAA compliance strategy.

What Is HIPAA and What Does It Mean to Healthcare Professionals?

On October 29, 1999, U.S. Department of Health and Human Services (DHHS) Secretary Donna E. Shalala proposed the first set of national standards geared toward protecting the privacy of Americans' personal health records. The standards meet one aspect of the requirements levied by HIPAA, (Public Law 104-191)) signed by President Clinton August 21, 1996.

Under HIPAA, all health plans, healthcare providers, and healthcare clearinghouses that maintain or transmit electronic data are required to ensure proper safeguards are in place for protecting the integrity and confidentiality of the information.

Never before has such legislation been enacted for securing the healthcare information maintained electronically. Initially, the law gave Congress up to 36 months to develop and pass privacy legislation. If not accomplished, then it would be up to the DHHS to promulgate the final set of regulations.

Congress did not meet its deadline, so the DHHS began publishing its proposed standards in 1999. To develop the standards, the administration worked with several public and private sector firms to put together the finest set possible.

"The standards outline specific rights for individuals regarding protected health information and obligations of healthcare providers, health plans, and healthcare clearinghouses."[1]

Prior to HIPAA, the security implemented to protect healthcare information was largely left to each organization. With a lack of strong management and organizational incentives, the level of information security provided was very disjointed and left many holes. For example, numerous hospitals would permit physicians to access the health records of patients who were not in their care.

[1] *HIPAA-iQ - Executive Summary, http://www.hipaa-iq.com/summary.html; September 7, 2000.*

"The privacy of Americans is protected in their bank transactions, their credit card statements, and even their video rentals. Yet, until today, Americans had no federal privacy protections for their medical records. These proposed standards are an important step forward in protecting the privacy of some of our most personal information."

—Secretary Donna E. Shalala, US Department of Health and Human Services

JCAHO Compliance Not Enough

The Joint Commission on Accreditation of Healthcare Organizations (JCAHO) did implement some standards to address information security through the accreditation process. However, the standards were not as specific as those outlined under HIPAA. Organizations in compliance with the Joint Commission standards will have a good start for meeting the rules levied by HIPAA, but most will still have much to do to be in full compliance with the newer regulations.

The issues raised by HIPAA must be addressed enterprise-wide, as each proposed rule carries with it certain legal, regulatory, process, security, and technology implications. The law will have a major, ongoing impact on healthcare providers in many areas, including resources, operations, and procedures. The law is quickly becoming a major issue for many healthcare organizations because the implementation timeframes are short and most organizations have not begun to prepare for the changes.

The Next Y2K—and the Clock Is Ticking

In addition, HIPAA compliance will be expensive. Overall costs associated with the changes required are estimated to be in the billions of dollars. The government has estimated the changes required for meeting the privacy regulation alone will be $3.8 billion.[2] "Industry experts estimate that HIPAA will be the next 'Y2K' in terms of resources and level of effort, and that annual healthcare expenditures for information security will increase from $2.2 million to $125 million over the next three years."[3]

Security needs vary per organization due to differences in size and complexity. However, certain HIPAA requirements must be addressed across all healthcare organizations, including the need to:

- Develop a written security policy
- Conduct security-related training for employees
- Ensure that physical access to all records is secured

Small health plans have 36 months to comply—by October, 2003.

Others must comply within 24 months—by October, 2002.

HIPAA is not intended to be a "one size fits all" policy, but rather, a carefully developed set of standards to protect sensitive medical information while affording the flexibility needed for each healthcare organization.

The "Administrative Simplification" aspect of HIPAA requires DHHS to develop standards and requirements for the maintenance and transmission of health information that identifies individual patients. The standards are designed to "improve the efficiency and effectiveness of the healthcare system by standardizing the interchange of electronic data for administrative and financial transactions; and protect the security and confidentiality of electronic health information."[4] The rules pertain to all healthcare organizations that maintain and transmit electronic data, regardless of size.

Once the final set of standards are adopted, small health plans will have 36 months to comply with the requirements, while others must comply within 24 months. Significant penalties will be levied on organizations that fail to comply within the required timeframe.

Stiff Penalties for Those Who Fail to Comply

For example, failure to comply with most of the requirements may lead to a fine of $100 per violation up to a maximum of $25,000. If an individual's healthcare information is wrongfully disclosed, much stiffer fines will be imposed. The penalty for a wrongful disclosure of information is $50,000, imprisonment of up to one year, or both. If the offense occurs as a result of false pretenses, the fine increases to $100,000, a prison sentence of up to five years, or both. If the offense occurs with the intent to sell the information, the penalty that may be imposed changes to $250,000 in fines, imprisonment of up to ten years, or both.

Several states have existing laws that govern the protection provided to medical information. The standards developed under HIPAA enhance the state law regulations. Note that in cases where the HIPAA standards and state law requirements are in conflict, the rules that provide a stronger level of protection are to prevail.

[2] *HIPAA-iQ - Executive Summary, http://www.hipaa-iq.com/summary.html; September 7, 2000.*
[3] *Information Security Management Handbook. Harold F. Tipton and Micki Krause ed. Auerbach Publications, 2000, p. 316.*
[4] *HIPAA-iQ - Executive Summary, http://www.hipaa-iq.com/summary.html; September 7, 2000.*

HIPAA: OFFENSE AND CONSEQUENCE

VIOLATION	PENALTY
Base violation of HIPAA requirements	• *$100 per offense* *Up to $25,000*
Wrongful disclosure of patient's health information	• *Up to $50,000* *One year imprisonment* *Or both*
Wrongful disclosure of patient's health information —under false pretense	• *$100,000 fine* *Five years' imprisonment* *Or both*
Intent to sell patient's health information	• *$250,000 fine* *Ten years' imprisonment* *Or both*

Failure to comply with HIPAA requirements could be very costly for organizations.

The Goal Is Simplification

Adherence to the standards outlined and implementation of appropriate safeguards are dependent upon numerous factors, such as existing configurations, risks and vulnerabilities inherent to a particular environment, and resources available. The standards were developed to be standards are designed to be nonvendor-specific, thus allowing organizations to implement the best products suited for their particular environments.

In addition, several issues are addressed by specific standards or regulations. These include:

- Privacy and security protections
- Electronic transmission of claims information
- Standard code sets
- The need for unique identifiers

HIPAA mandates that the new security standards will be geared toward protecting patient records, while permitting appropriate access by healthcare providers and others who need it. The goal is to provide a level of "administrative simplification" while ensuring thorough protection is provided to maintain the confidentiality of patient information.

HIPAA will have a major impact on healthcare organizations, most of whom have done little work previously to address confidentiality issues.

Major HIPAA Security Requirement Categories

Note that the standards apply to healthcare information in **electronic form only**. They do not address the security of patient records and healthcare transactions processed in hardcopy or paper format.

The privacy regulations prohibit healthcare providers, health plans, and clearinghouses to use or disclose health information that identifies an individual without the patient's consent or as otherwise permitted under the regulations. The protection begins once the information becomes electronic and remains in force while the information is maintained by the healthcare organization.

If the health information does not identify a specific individual, then the information may be used in any way the organization chooses provided it cannot identify a particular person.

DHHS divided the security requirements into several distinct groups: administrative procedures, physical safeguards, and technical data security services:[5]

- **Administrative procedures** focus on the development and implementation of security policies used to guard data integrity, confidentiality, and accessibility
- **Physical safeguards** address devices and measures that are part of the information infrastructure. This includes physical computer systems, locks, environmental hazards, building access, location of servers, etc.
- **Technical data security services** include the actual processes that guard, control, and monitor access to the information systems, and the technical security mechanisms refer to the devices used to protect the information as it is transmitted over a network.

Micki Krause provides a summary of some of the various procedures that must be adhered to in the *Information Security Management Handbook*, 4th edition.[6] The following points were abstracted from the author's summary and provide a good working list of some of the many issues healthcare organizations must consider.

[5] *A fourth category is Technical Security Mechanisms, which for purposes of this white paper, have been included in Technical Data Security Services.*
[6] *Information Security Management Handbook. Harold F. Tipton and Micki Krause ed. Auerbach Publications, 2000, pp. 316-319..*

HIPAA COMPLIANCE ISSUES

Organizational and Administrative Procedures

Ensure organizational structures exist to develop and implement an information security program

The Chief Security Officer is responsible for the development of policies to control access to and for the release of, individually identifiable patient healthcare information. This executive must:

- Establish a security certification review¨
- Establish policies and procedures for the receipt, storage, processing, and distribution of information
- Develop a contractual agreement with all business partners, ensuring confidentiality and data integrity of exchanged information
- Ensure access controls that provide for an assurance that only those persons with a need can access specific information.
- Implement personnel security, including clearance policies and procedures
- Perform security training for all personnel
- Provide for disaster recovery and business resumption planning for critical systems, applications, and networks.
- Document policies and procedures for the installation, networking, maintenance, and security testing of all hardware and software
- Establish system auditing policies and procedures
- Develop termination procedures which ensure that involuntarily terminated personnel are immediately removed from accessing systems and networks and voluntarily terminated personnel are removed from systems and networks in an expedient manner ¨
- Document security violation reporting policies and procedures and sanctions for violations

Physical Security Safeguards

- Establish policies and procedures for the control of media (e.g., disks, tapes), including activity tracking and data backup, storage, and disposal
- Secure work stations and implement automatic logout after a specified period of nonuse

Technical Data Security Measures

- Assure that sensitive information is altered or destroyed only by authorized personnel
- Provide the ability to properly identify and authenticate users
- Create audit records whenever users inquire or update records
- Provide for access controls that are transaction-, role-, or user-based
- Implement controls to ensure that transmitted information has not been corrupted
- Implement message authentication to validate that a message is received unchanged
- Implement encryption or access controls, including audit trails, entity authentication, and mechanisms for detecting and reporting unauthorized activity in the network

Healthcare professionals have many issues to consider—and a short timeframe in which to develop and implement a strategy for HIPAA compliance. Much of the work will be policy- and technology-related as organizations scramble to revamp their medical processing systems to protect patients' health information privacy.

Unfortunately, No Common Electronic Data Transmittal Standards Yet

As with the other areas addressed by HIPAA, there has not been a common standard for the electronic transmission of healthcare transactions between healthcare providers and the organizations that pay the claims. Payers will now be required to accept specific, common standards used for Electronic Data Interchange (EDI).

For example, claims, eligibility verifications, enrollment, and related transactions must now comply with the American National Standards Institute ANSI X12N standards. Similar requirements exist for pharmacy transactions, diagnoses and inpatient hospital services, medical procedures, and physician services.

The regulations governing the electronic transmission of patient claims apply to all forms of electronic storage and transmission media that may be used to complete transactions (e.g., tapes, CDs, dial-up lines, private networks, etc.).

In addition, organizations choosing to transmit data that pertains to an individual over the Internet must also comply with the signature standard. The purpose of the Electronic Signature Standard is to provide a reliable method for ensuring data integrity, non-repudiation, and user authentication. HIPAA does not mandate the electronic transmission of healthcare transactions. It simply requires these specific standards be adhered to for organizations that choose to use EDI.

Industry experts estimate that HIPAA will be the next 'Y2K' in terms of resources and level of effort, and that annual healthcare expenditures for information security will increase from $2.2 million to $125 million over the next three years.

Standard Identification Numbers On the Way

With a lack of standards industry-wide, healthcare organizations have developed numerous methods for tracking patients and claims over the years. HIPAA addresses the need to standardize the identification numbers or symbols used through the use of unique identifiers for providers, health plans, employers, and patients.

The unique identifier used for providers and health plans is expected to be based on the identification codes previously developed for use with the Medicare system. Both codes will be ten numeric digits, with the tenth position containing a check code. Note that the provider code is also referred to as the National Provider Identifier or NPI.

Since the Internal Revenue Service has already developed unique identification codes to denote specific employers, the Employer Identification Number (EIN) is expected to be the standard used for the employer identifier. The standard regarding the identification of individual patients remains to be addressed. This standard has been very controversial and is currently held up pending privacy legislation. However, it too is expected to be ten numeric digits in length, with the final digit serving as a check code.

All of the proposed identification standards are available on the Internet and may be downloaded from http://aspe.os.dhhs.gov/admnsimp/.

Nine Critical Steps in HIPAA Compliance Planning

Healthcare organizations should begin preparing to implement the changes required by HIPAA, if they have not done so already. Here are some useful guidelines to help them get started:

1. Obtain a copy of the regulations and compare the rules to your organization's current practices and policies. Several web sites outline different aspects of the law and provide automatic e-mail notifications when a new posting appears. Some of the web sites providing up to date information on HIPAA include:

- **http://www.hcfa.gov/regs/hipaacer.html**
- **http://hippo.findlaw.com/hipaa.html**
- **http://www.hcfa.gov/hipaa/hipaahm.htm**
- **http://www.dol.gov/dol/pwba/public/pubs/hipatim.htm**
- **http://www.dhhs.gov/**

2. Identify your HIPAA compliance team. These individuals should be responsible for measures taken to ensure compliance with the legislation are addressed clearly in the organization's strategic plans, budgets, and vendor contracts.

3. Review existing security policies and procedures. Update them where necessary.

4. Perform a complete inventory of all information resources and systems that contain individual medical information.

5. Conduct a risk assessment to identify potential vulnerabilities to those systems.

6. Develop an action plan to repair any patient information security risks. Identify the greatest risks first.

7. Review patient indexes or databases to ensure unique identification numbers are used for all clients.

8. Correct duplicate identification numbers or numbers representing more than one patient.

9. Finally, review auditing capabilities to ensure an acceptable level of monitoring is provided. At a minimum, every access to every information system should be recorded.

GNTS Information Assurance experts can work with healthcare organizations to identify potential threats and ensure systems are updated appropriately for HIPAA compliance.

How HIPAA Security Professionals Can Ease the Burden

While the nine steps listed above form a solid foundation for HIPAA compliance, many organizations are simply too overworked already, and will need help achieving compliance. As a result, many will turn to strategic outsourcing to implement their HIPAA compliance programs. Outsourcing offers several advantages, including:

- Knowledgeable experts, trained in the nuances of HIPAA
- Proven methodologies that can shorten development and execution of a HIPAA compliance program
- Cost-effective methods that allow busy healthcare professionals to keep their focus on core business activities

Taking a holistic approach to computer security, Global*Network* Technology Services (GNTS) is an example of an outsourcing solution that can help overworked healthcare organizations achieve HIPAA compliance. GNTS Information Assurance Assessment (IAA) service provides a risk assessment which addresses system design, configuration settings, and policies.

GNTS Information Assurance experts can work with healthcare organizations to identify potential threats and ensure systems are updated appropriately for compliance with HIPAA legislation. This includes:

- **Security policies and disaster recovery plan reviews**—To ensure best practices are implemented in compliance with specific HIPAA rules and regulations, GNTS will work with customers to develop or enhance security policies and disaster recovery plans as they relate to HIPAA regulations.
- **Penetration testing and war dialing**—This examines the overall information infrastructure, then identifies vulnerabilities that may be exploited by either internal or external sources.
- **IT implementation**—Once all discrepancies have been identified, Global*Network* Technology Services Information Assurance specialists will work with the organization's Information Technology (IT) staff to implement required changes.
- **HIPAA security training for employees —** A GNTS Information Assurance specialist can also help ensure the appropriate level of employee training is provided through the Information Assurance Awareness Education (IAAE) service. Thorough employee training enables organizations to address what is typically the greatest threat first—lack of user awareness.

Summary: HIPAA Deadlines Are Fast-Approaching

The healthcare industry has been involved with an expansive move to computerize health records and other sensitive information. This coupled with an increased number of enterprise wide solutions and remote connectivity, has resulted in a need for thorough direction regarding the security provided to the sensitive information maintained on these systems.

Healthcare organizations can achieve the proper level of security to ensure confidentiality, integrity, and availability requirements are met through proper planning and the use of existing technology. However, they must begin preparing now. The regulations have a very short turnaround time and carry stiff penalties for non-compliance.

HIPAA compliance is attainable—but only if healthcare organizations get started now. The fastest, most cost-effective way to get there is to outsource key tasks to HIPAA Information Assurance experts.

Get ready—HIPAA will have significant impact on healthcare professionals. Begin by:

- Learning the regulations and assessing the information infrastructure for compliance requirements is the best place to begin preparing for HIPAA.
- Working with HIPAA security experts who can help design and implement a proven compliance strategy that meets the three major requirements (written security policies, employee training, and secured physical access to patient records).

For more information about HIPAA and what it will mean to your organization, contact your GNTS representative or authorized reseller. Or visit us on the Web at www.globalnts.com.