

Healthcare and the Internet: The Impact of HIPAA Privacy and Security Rules and Other Privacy and Electronic Commerce Developments on the Healthcare Market

September 15, 2000

Randall M. Whitmeyer*

The United States, including its healthcare industry, has been an early and enthusiastic adopter of information technology and communications advances -- especially the Internet -- with the overall goal of improving productivity. However, as more sensitive personal information makes its way into electronic form, and as more of this information is transmitted between and among organizations over the Internet, privacy concerns have risen to a fever pitch.

Concern over the protection and use of personal information is not new. With virtually every new technology and communications device, there has been discussion regarding the ramifications to personal privacy. As far back as 1891, a law review article on privacy stated that: "Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'" In addition, around 25 years ago, concern over computer and database advances led a federal commission to conclude: "Neither law nor technology gives an individual the tools he needs to protect himself from the undesired difficulties a record can create for him--and may also leave him helpless to stop damage once it has started. Current law is neither strong enough nor specific enough to solve the problems that now exist."

Has the battle for privacy protection in the United States been lost? Unlike many other countries, the United States lacks comprehensive individual data protection laws and regulations. Instead, a patchwork of federal and state laws exist that cover specific subject areas (including widely varying state statutes and rules regarding medical information) only. In 1999, Scott McNealy, Chief Executive Officer at noted hardware and software vendor Sun Microsystems, was quoted as saying "You have no privacy. Get over it."

In the healthcare field, at least, Congress has indicated a clear intent to establish protections for the privacy of electronic patient records. In 1996, Congress included certain "administrative simplification provisions" in the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"; 42 U.S.C. §1320d) in order to address the twin goals of encouraging the use of electronic transactions to increase efficiency and decrease

* Partner, Hutchison & Mason PLLC, Raleigh, North Carolina.
rwhitmeyer@hutchlaw.com. 919-829-4319

costs in the health care field, while at the same time establishing a baseline of privacy protections for individually identifiable patient information. HIPAA and its associated regulations promise to cause health care providers, health plans and service providers to restructure, at a heavy cost, their information handling processes and technology.

This article will:

- Review the recent final HIPAA rule on Standards for Electronic Transactions (the "Electronic Transactions Rule") promulgated on August 17, 2000 by the Department of Health and Human Services ("HHS"). This first final rule, while generally limited to electronic transaction standards, contains a number of important definitions and requirements as well as some clues regarding how the agency will address criticism of the more controversial privacy and security standards it has proposed over the last 24 months.
- Review the proposed HIPAA regulations relating to privacy issued November 3, 1999 (the "Proposed Privacy Rule") and to security issued August 12, 1998 (the "Proposed Security Rule").
- Briefly summarize other recently-enacted privacy and e-commerce/computer laws and regulations that may impact the health care industry.
- Conclude with some practical suggestions for the healthcare organization and service providers for managing risk in light of these new "information era" legal rules and technological developments.

Unfortunately, this article will of necessity have a somewhat short shelf life, given the new rules and laws that are likely to be implemented in the next few years. To stay current, you should consider regularly checking the following web sites (among your other favorites):

- www.healthprivacy.org. Georgetown University's health privacy project. Many good resources, including a 50-state survey (as of July 1999) of state medical record privacy laws.
- <http://aspe.os.dhhs.gov/admnsimp/>. The Department of Health and Human Service's portal on HIPAA rules. The text of all proposed and final HIPAA rules is contained here. Sign up for the listserv and be notified when proposed and final rules are issued by the HHS.
- www.cdt.org. The Center for Democracy and Technology. A well-respected and fairly balanced organization dedicated to privacy, free speech and related issues.

A. THE HIPAA ELECTRONIC TRANSACTIONS RULE

The Electronic Transactions Rule establishes required transaction codes and formats for the following healthcare-related transactions: health care claims or equivalent encounter information; eligibility for a health plan; referral certification and authorization; health care claim status; enrollment and disenrollment in a health plan; health care payment and remittance advice; health plan premium payments; and coordination of benefits. The Rule establishes specific published standards (primarily ANSI ASC X12N, Version 4010) in each of these transaction areas. Standards for first report of injury and claims attachment transactions (also required by HIPAA) have been deferred by the HHS to a later date.

The following key dates are established by the Electronic Transactions Rule:

August 17, 2000	Publication of Final Rule in Federal Register
October 16, 2000	Effective Date of Rule
October 16, 2002	Compliance Date for Health Care Providers, Health Care Clearinghouses, and Health Care Plans other than “Small Health Care Plans”
October 16, 2003	Compliance Date for Small Health Care Plans

In the Federal Register notice, the HHS includes the following important note regarding the timing for implementation of the Electronic Transactions Rule:

The Secretary has developed this rule in conjunction with the development of standards to protect the privacy of individually identifiable health information, including information that will be transmitted pursuant to these transaction standards. Compliance with the privacy standards will be required at approximately the same time as compliance dates of this rule. If the privacy standards are substantially delayed, or if Congress fails to adopt comprehensive and effective privacy standards that supercede the standards we are developing, we would seriously consider suspending the application of the transaction standards or taking action to withdraw this rule.

Based on this comment, the HHS is likely to publish final security and privacy rules with similar compliance dates very shortly. However, the HHS puts Congress and industry participants “on notice” that the benefits of standardization on electronic formats will be delayed if there is continued resistance to proposed privacy and security regulations. In any event, health care companies and plans will need to make required changes and improvements in their technology, policies, and procedures well in advance of any

established deadlines in order to allow time for testing and review of technology and preparation and printing of required policies and notices.

HIPAA applies generally to the following "covered entities": (a) health plans, (b) health care clearinghouses, and (c) health care providers that transmit any health information in electronic form in connection with one of the transactions referred to above. These terms are defined in HIPAA, but (slightly different) definitions are also included in the Electronic Transactions Rule. However, the HHS states in its comments that it is deferring revision of the definition of a health care provider until the final rule for Standard Health Care Provider Identifiers is issued. Also, in the final Electronic Transactions Rule, the HHS changed the definition of a "small health plan" from the definition in the proposed Rule to mean a health plan with annual receipts of \$5 million or less.

As a general rule, the Electronic Transactions Rule requires that, for any transaction between covered entities conducted using electronic media for which the HHS has adopted a standard under the Rule (including transactions *within* the covered entity—a change from the proposed Rule), each covered entity must conduct the transaction as a standard transaction—i.e., using the standard formats and content set forth in the Electronic Transactions Rule. In addition, if a covered entity uses a "business associate" to conduct all or part of a covered transaction, then the covered entity must require (by contract) the business associate to do the following: (1) comply with all applicable requirements of the Rule, and (2) require any agent or subcontractor to comply with all applicable requirements of the Rule. The final Electronic Transactions Rule also adds a limited exception for health care providers: If the provider uses direct data entry to conduct a transaction with a health plan, then the provider is not required to use the "format" requirements of the standard, although the provider is still required to meet the applicable data content and data conditions requirements of the standard.

Because HIPAA is concerned with the adoption of national standards to enable the electronic exchange of health information, the HIPAA regulations generally do not apply to purely paper transactions. The Electronic Transactions Rule does not require health care providers to send or accept electronic transactions (although, it appears possible that by contract a health plan could make such a requirement). However, a health plan *is required* to accept electronic transactions in standard format when requested by any entity (whether or not a covered entity). The Electronic Transactions Rule contains a number of specific rules that require a health plan to accept transaction data in standard electronic format and not discriminate against covered entities using standard formats.

The comments in the Federal Register contain several detailed examples that are helpful in understanding the meaning of the Rule in various contexts.

Under Section 1320d-5 of HIPAA, the HHS is required to impose penalties of not more than \$100 per violation on any person who fails to comply with a standard, except that the total amount imposed on any one person in each calendar year may not exceed

\$25,000 for violations of an identical requirement or prohibition during a calendar year.
Penalties will not apply:

- If it is established to the satisfaction of the Secretary that a person did not know, or by exercising reasonable diligence would not have known, that the person violated the provision.
- If: (i) the failure to comply was due to reasonable cause and not to willful neglect; and (ii) the failure is corrected during a 30-day cure period.
- If the failure was due to reasonable cause and not to willful neglect, the penalty may be waived to the extent that the payment of such penalty would be excessive relative to the compliance failure involved.

In the Electronic Transactions Rule, the HHS included the following statements regarding remedies and enforcement:

[W]e will be developing a separate compliance and enforcement rule to establish compliance and enforcement procedures for these and other administrative simplification requirements. We plan to publish an NPRM requesting public comments next year, and to subsequently issue a final compliance and enforcement regulation that will become effective prior to the first compliance dates of these rules. We anticipate addressing the specific issues of compliance, timing, appeals, and technical assistance in the projected compliance and enforcement rulemaking. We also plan to address the practicability of using some type of self-certification or certification by external parties to demonstrate compliance with some or all of the requirements.

We encourage covered entities, trading partners and business associates to address issues relating to compliance and resolution of disputes concerning use of these standards in their trading partner agreements.

In other words, more to come!

B. THE PROPOSED PRIVACY RULE

The Proposed Privacy Rule is a detailed commentary and set of proposed rules to implement HIPAA's directive that (if Congress did not otherwise act) HHS take action to protect individually identifiable health information. The Rule applies to any covered entity that possesses protected health information ("PHI"), as defined below, as well as in many respect to business partners that possess PHI through a contract with a covered entity. Despite its detail and length, the Proposed Privacy Rule does not pre-empt state

laws imposing stricter privacy rules. It is intended to create a floor, not a ceiling, on privacy restrictions on medical records.

1. Disclosure Rules and Restrictions

Protected Health Information (“PHI”) means health care-related information, including demographic information, regarding an individual that: (i) identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual; and (ii) either is or has been at some point in electronic format. Individually identifiable health information that has never been placed into electronic format would not be subject to the restrictions of the Proposed Privacy Rule.

The HHS has requested comments whether the Rule should be extended to all individually identifiable health information, regardless of whether it had ever been put into electronic format.

Under the Proposed Privacy Rule, covered entities may disclose PHI only if: (a) the patient has provided written authorization (the Rule contains specific procedural and substantive requirements regarding such authorizations); (b) the purpose of the disclosure is to provide health care treatment for the patient, process payment information, or for internal health care operations; or (c) in other specified contexts. The term “health care operations” includes activities such as peer review and student training; quality assessment and improvement activities; insurance rating and other insurance activities; fraud and abuse detection; and compiling and analyzing information in anticipation of a legal proceeding. The other specified contexts in which disclosure of PHI is allowed without written authorization include:

- For public health activities, generally to a public health authority
- For health oversight activities authorized by law, such as required to determine if institutions are complying with applicable program standards
- For judicial and administrative proceedings
- For disclosures to coroners and medical examiners
- For disclosures to law enforcement officials, under a number of specified circumstances
- For disclosures and uses by government agencies, if for inclusion in a system that collects data in support of lawful policy, planning, regulatory or management functions
- For limited disclosures in a health care provider’s patient directory

- For banking and payment processes, in connection with routine banking activities or payment
- For research purposes, if approved in a signed waiver by an Institutional Review Board or a privacy board
- In emergency circumstances
- For disclosures to next-of-kin
- For specialized classes (military personnel, veterans, intelligence community, and Department of State) in certain identified circumstances
- Where use or disclosure is required by law

The Rule also specifies a non-exclusive list of examples where written authorization of the individual would be required:

- Use for marketing of health and non-health items and services by the covered entity;
- Disclosure by sale, rental, or barter;
- Use and disclosure to non-health related divisions of the covered entity, e.g., for use in marketing life or casualty insurance or banking services;
- Disclosure, prior to an individual's enrollment in a health plan, to the health plan or health care provider for making eligibility or enrollment determinations relating to the individual or for underwriting or risk rating determinations;
- Disclosure to an employer for use in employment determinations; and
- Use or disclosure for fundraising purposes

A covered entity may not condition the provision of treatment or payment on the provision by the individual of a requested authorization for use or disclosure, except where the authorization is requested in connection with a clinical trial.

In general, a covered entity must make all reasonable efforts not to use or disclose more than the minimum amount of PHI necessary to accomplish the intended purpose of the use or disclosure. To comply with this standard, a covered entity must, among other things, identify appropriate persons within its organization to determine what information should be used or disclosed consistent with the minimum necessary standard.

The requirements of the Proposed Privacy Rule do not apply to PHI that a covered entity has “de-identified.” Information is presumed not to be individually identifiable (i.e., de-identified) if: (A) the following identifiers have been removed or concealed: (1) name; (2) address, including street address, city, county, zip code, and equivalent geocodes; (3) names of relatives; (4) names of employers; (5) birth date; (6) telephone numbers; (7) fax numbers; (8) e-mail addresses; (9) social security number; (10) medical record number; (11) health plan beneficiary number; (12) account number; (13) certificate/license number; (14) any vehicle or other device serial number; (15) Web URL; (16) Internet Protocol address; (17) finger or voice prints; (18) photographic images; and (19) any other unique identifying number, characteristic or code; and (B) the covered entity has no reason to believe that any anticipated recipient of such information could use the information alone or in combination with other information, to identify an individual.

2. Patient Rights

With certain exceptions, an individual has a right to access, including a right to inspect and obtain a copy of, his or her PHI from health care providers or health care plans, including their business partners if not a duplicate of information stored by the provider or by the plan (but not from health care clearinghouses). The covered entity must follow specified procedures in connection with individual’s seeking access to his or her PHI (including responding to requests for access within at least 30 days). If access is denied based on an enumerated exception, the covered entity must provide the individual with a written statement in plain language of the basis for the refusal, along with a description of both an internal appeal process and how to file a complaint with the HHS.

An individual also has the right to request a covered entity that is a health care plan or a health care provider to correct PHI about him or her for as long as the covered entity maintains the information. The covered entity must have procedures in place to make this request, whether it should be denied or granted, and to distribute amendments and corrections to its business partners and others to whom incorrect information has been disclosed. The covered entity may deny a request for correction if it determines that the information that is the subject of the request: (a) was not created by the covered entity; (b) would not be subject to access by the individual, as described above; or (c) is in fact accurate and complete. The Rule sets forth a number of administrative procedures associated with the above right of correction.

Another right granted to individuals by the Proposed Privacy Rule is the right to receive an accounting of all disclosures of protected PHI made by a covered entity as long as such PHI is maintained by the entity, except for disclosures (1) for treatment, payment and health care operations; and (2) to health oversight or law enforcement agencies, if such agency has provided a written request stating that the exclusion is necessary because disclosure would be reasonably likely to impede the agency’s activities and specifying the time for which such exclusion is required.

An individual also may request that certain uses or disclosure of PHI by the covered entity that would otherwise be allowed under the Proposed Privacy Rule be restricted. The covered entity is not required to agree to a requested restriction.

3. Other Covered Entity Requirements

Except for disclosures made between health care providers for consultation or referral purposes, a covered entity may not disclose PHI to a business partner without satisfactory assurance from the business partner that it will appropriately safeguard the information. In addition, a covered entity must take reasonable steps to ensure that its business partners comply with the requirements of the Proposed Privacy Rule with respect to all tasks and activities it performs on behalf of the entity, to the extent the covered entity would be required to comply with such requirements. “Satisfactory assurance” is defined to mean a contract between the covered entity and the business partner that provides that the business partner will:

- Not use or further disclose the information other than as permitted or required by the contract;
- Not use or further disclose the information in a manner that would violate the requirements of the Proposed Privacy Rule, if done by the covered entity;
- Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by its contract;
- Report to the covered entity any use or disclosure of the information not provided for by its contract of which it becomes aware;
- Ensure that any subcontractors or agents to whom its provides PHI received from the covered entity agree to the same restrictions and conditions that apply to the business partner with respect to such information;
- Make available PHI in accordance with the patient access rights described in the Proposed Privacy Rule;
- Make its internal practices, books and records relating to the use and disclosure of PHI received from the covered entity available to the HHS for purposes of determining the covered entity’s compliance with the Rule;
- At termination of the contract, return or destroy all PHI received from the covered entity that the business partner still maintains in any form and retain no copies of such PHI; and

- Incorporate any amendment or corrections to PHI when notified pursuant to the patient correction provisions of the Rule

The contract between the business partner and covered entity must also: (a) state that individuals whose PHI is disclosed under the contract are intended third-party beneficiaries of the contract (this is likely to be challenged as outside the scope of the HHS' authority, since no private right of action is allowed under HIPAA); and (b) authorize the covered entity to terminate the contract if the business partner violates a material term of the contract required by the Rule.

A covered entity that is a health care plan or health care provider is also required to provide adequate notice of its policies and procedures with respect to PHI to individuals.

This notice must include in plain language the uses and disclosures to be made of the PHI without individual authorization, with a distinction between uses and disclosures required by law and uses and disclosures permitted but not required by law. In addition, the notice must state:

- That other uses and disclosures will be made only with the individual's authorization and such authorization may be revoked;
- That an individual has the right to request, and a description of the procedures for exercising this right, the following with respect to his or her PHI: (1) inspection and copying; (2) amendment or correction; and (3) an accounting of the disclosures of such information by the covered entity;
- That the covered entity is required by law to protect the privacy of its individually identifiable health information, provide a notice of its policies and procedures with respect to such information, and abide by the terms of the notice currently in effect;
- That the entity may change its policies and procedures relating to PHI at any time, with a description of how individuals will be informed of material changes;
- That individuals may complain to the covered entity and to the HHS if they believe that their privacy rights have been violated;
- Who the entity's privacy contact person or office is; and
- The date the version of the notice was produced.

Copies of the notice must be made available by covered entities on request. In addition, health plans must make the notice available: (a) as of the date of compliance with the Rule; (b) upon enrollment; (c) within 60 days after revisions; and (d) no less frequently than once every three years. Health care providers must make the notice available: at

the first service delivery, and by posting a copy of the notice in a clear and prominent location.

Each covered entity is required to appoint a privacy official responsible for the development and operation of the privacy policies and procedures of the entity. In addition, the covered entity must designate a contact person or office who is responsible for receiving complaints under the Rule and who is able to provide further information about the privacy notice described above. Training on relevant privacy policies and procedures must be provided to all members of the covered entity's workforce who are likely to obtain access to PHI.

A covered entity must have administrative, technical and physical procedures in place to protect the privacy of PHI. Such procedures must include adequate procedures for verification of the identity and/or authority, as required in the Rule, of persons requesting such information, where such identity or authority is not known to the entity.

A covered entity must adequately document its compliance with the Proposed Privacy Rule. The Proposed Privacy Rule contains an exhaustive list of the types of documentation that the entity should be prepared to make available. The covered entity must maintain specified documentation for six years. The entity must also submit compliance reports as deemed necessary by HHS, cooperate with HHS if it undertakes a review of the entity's relevant policies and procedures, permit HHS access to pertinent information regarding its compliance, and refrain from intimidating or retaliatory acts.

4. Penalties

Under 42 U.S.C. Section 1320d-6 of HIPAA, a person who knowingly obtains or discloses individually identifiable health information in violation of HIPAA shall: (1) be fined not more than \$50,000, imprisoned not more than 1 year, or both; (2) if the offense is committed under false pretenses, be fined not more than \$100,000, imprisoned not more than 5 years, or both; and (3) if the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, be fined not more than \$250,000, imprisoned not more than 10 years, or both.

C. THE PROPOSED SECURITY RULE

Under HIPAA, the HHS is charged with adopting security standards that take into account: (1) the technical capabilities of record systems used to maintain health information; (2) the costs of security measures; (3) the need for training persons who have access to health information; (4) the value of audit trails in computerized record systems; and (5) the needs and capabilities of small health care providers. The Proposed Security Rule, which also discusses electronic signature requirements, describes

administrative, technical and physical safeguards and associated policies and procedures that covered entities would be required to implement. The proposed standards are general and technology-neutral.

Under the Proposed Security Rule, covered entities must assess potential risks and vulnerabilities to individual health data in its possession and develop, implement and maintain appropriate security measures that are documented and kept current.

1. Administrative Procedures

- Certification that computer systems and networks meet established security policies and standards
- A chain of trust agreement between business partners for the protection of data.
- A contingency plan for dealing with system emergencies including:
 - assessment of the sensitivity, vulnerabilities, and security of the health care information
 - a data backup plan
 - a disaster recovery plan
 - an emergency operation plan
 - testing and revision procedures
- A formal records processing mechanism
- Policies regarding access to information, including:
 - Access authorization
 - Access establishment
 - Access modification
- Internal auditing of system activity and audit trails
- Personnel security provisions, including
 - Procedures for supervision of maintenance personnel
 - Record of access authorizations
 - Access authorization for maintenance and operational personnel
 - Personnel clearance procedures
 - Personnel security policies and procedures
 - Security training
- Security configuration management
 - Documentation of security plans
 - Security procedures for new system installations and maintenance

- Inventory of hardware and software assets
- Security testing
- Virus checking
- Reporting procedures to document security incidents
- Security management
 - Risk analysis and management
 - Security policy and employee sanctions
- Termination procedures, including
 - Changing locks
 - Removal from access lists
 - Removal of user accounts
 - Collection of keys and other forms of access.
- Security Training
 - Security awareness training
 - Periodic security reminders
 - Education concerning virus protection
 - Education regarding monitoring log-in attempts
 - Education in password management

2. Physical Security Requirements

- Assignment of security responsibilities
- Media controls regarding the receipt and removal of hardware and software from the facility, including:
 - Access control
 - Accountability for tracing removed property
 - A data backup, storage, and disposal system
- Physical access controls, including:
 - Disaster data recovery plan
 - Emergency mode operation plan
 - Equipment control into and out of the facility
 - Facility security plan
 - Authorization procedures for granting access
 - Maintenance records
 - Need-to-know procedures for personnel access
 - Visitor sign-in and sign-out procedures
 - System testing and revision procedures

- Policies on workstation use
- Secure workstation location
- Security awareness training

3. Technical Security Services

- Access Control, including
 - a procedure for emergency access
 - context-based access, role-based access, or user-based access
 - optional use of encryption
- Audit controls to examine system activity
- Authorization controls, including either role-based access or user-based access
- Data authentication
- Entity authentication, including:
 - Automatic logoff
 - Unique user ID
 - At least one of the following features: biometric identification; password; personal id number; telephone callback procedure; or token

4. Technical Security Mechanisms

If the entity uses communications or an electronic network, the following security mechanisms are required:

- Integrity controls
- Message authentication
- Either access controls or encryption

If the entity uses an electronic network, the following security mechanisms are required:

- An alarm system to detect abnormal conditions
- An audit trail
- Entity authentication
- Event reporting of operational irregularities

5. Electronic Signature Standard

The Proposed Security Rule does not independently require the use of an electronic or digital signature. However, if a covered entity elects to use an electronic signature, or if a transaction standard adopted by the HHS requires an electronic signature, the following standards shall apply:

- The standard for electronic signatures is a digital signature, which is an electronic signature based upon cryptographic methods of originator authentication, computed using a set of rules and parameters so that the identity of the signer and the integrity of the data can be verified
- The signature method must assure all of the following features:
 - Message integrity
 - Nonrepudiation
 - User authentication

D. OTHER PRIVACY AND E-COMMERCE/COMPUTER LAWS

1. Personal Information Collected On-line

HIPAA applies to certain transactions and the protection of personally identifiable health information, without discussing directly the issue of data collected from the general public through web sites. Of course, any PHI collected through a web site by a covered entity would be subject to the HIPAA rules. Other types of personal information, however, would not be covered. Although there are no generally applicable laws regarding the collection of personal information on-line, the Federal Trade Commission has been actively studying and reporting on on-line privacy issues over the last three years. In May 2000, the FTC reversed its long held position on privacy standards, and decided to encourage federal regulation on privacy matters. The reversal resulted from a survey that found that most on-line operators were not adequately protecting the privacy of identifiable information on the Internet. The FTC has also undertaken several investigative and enforcement action based on complaints that web-sites and on-line advertisers have failed to abide by their published Web privacy policies. In addition, the FTC recently executed an understanding with the leading on-line advertising servers regarding the permitted acquisition and merger of consumer information collected on-line by companies such as Doubleclick.

The legal staff of a health care organization should regularly review the functions being performed by and information collected on its web sites, both by the organization itself and its affiliates and advertising partners. Privacy policies and web disclaimers should be updated as necessary.

2. The Children's Online Privacy Protection Act

The Children's Online Privacy Protection Act, 47 U.S.C. §231 ("COPPA") regulates the use and collection of children's identifiable information as they participate on the

Internet. However, barely two months after its effective date, the Third Circuit held that COPPA was an unconstitutional restriction on free speech and invalidated the law. *ACLU v. Reno*, No. 99-1324 (3rd Cir. June 22, 2000). Health care organizations that maintain web sites that are intended for children or children's health issues may nevertheless wish to comply with its regulations. Commercial Web Site operators who target children are required to obtain verifiable parental consent before collecting, using, or disclosing personal information of children under the age of 13.

Under COPPA, web site operators must post a privacy notice designed to make parents aware of the collection of personal information. There must be a separate, clear, and explicit link to the policy on the home page and any area where children's information is collected. Included in the notice must be the name and contact information of the web site operator, the types of personal information collected, how the information is used, and whether disclosure to third parties occurs.

The notice must also inform parents that they can review and have deleted the child's personal information, and refuse to permit the further collection of the information. The notice must also include a statement alerting the parents to the operators' prohibition from conditioning a child's participation in activity on the child's disclosing more information than is reasonably necessary.

COPPA and its implementing regulation proscribes different methods of verifiable consent for differing types of collected information. More reliable methods of consent will be required for those activities which pose the greatest safety and privacy risks. Typically, chat rooms, disclosure to third parties, and other interactive activities are the targeted risks that require more reliable forms of consent. Operators should provide methods of obtaining consent through non-electronic means in high-risk areas.

Internal uses of information are allowed with verifiable and continued parental consent. Companies will be responsible for implementing systems to ensure compliance with this regulation until more reliable methods of verification are developed. With the advent of new signature technologies, companies will be required to upgrade their current systems within the two-year window proscribed by the statute.

The following activities do not require Parental Consent under COPPA:

- Contact information that is used for one time only response to a specific request by the child. The information cannot be stored and reused to contact the child.
- A request for the name or the contact information of a parent or child that is used for the sole purpose of obtaining parental consent is allowed. This information cannot be stored or maintained in a retrievable format.

3. The Gramm-Leach-Bliley Financial Privacy Act

Title V of the Gramm Leach Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (“the Act”) regulates privacy issues for financial institutions. Under the final regulation promulgated under the Act, the effective date for compliance has been delayed to July 1, 2001. It requires financial institutions to create, disclose, and maintain a privacy policy for their customers and allow them to opt out before disclosing their non-public personal information to third parties. The notice must be provided to each of the company’s customers at the inception of the customer relationship and annually. The Act does not apply to businesses or parties who obtain financial products for business purposes.

The Act applies to any identifiable personal information, financial or otherwise. If the information is reasonably believed to be public information, then the financial institution may disclose it. Many broad categories fall under this exception: public records, telephone directories, widely distributed media, etc. However if an individual can control the information, then the institution should not assume that it is publicly available. Disclosure can only occur if the existence of a customer relationship that is not public is not disclosed. Privacy is afforded to all personal information collected by a financial institution regardless of whether the individual becomes a customer of the institution.

4. European Union Data Protection Directive

In 1995, the European Union (EU) adopted a comprehensive personal data protection scheme designed to afford its citizens privacy protections. EU Directive 95/46/EC regulates the collection and disbursement of identifiable personal information within the 15 membership countries. The directive primarily requires operators to give users notice of personal information collection and to require the users to give permission for future use of the collected data. One provision of the directive forbids the transfer of personal information to countries with inadequate privacy protections, causing concern about U. S. companies doing business on-line and/or with European consumers or companies. In an attempt to mollify the EU and promote U. S. commerce, the United States and the EU entered into negotiations to sort out the differences between U. S. interests and the EU.

On July 27, 2000, the European Union approved safe harbor provisions resulting from these negotiations that are designed to afford U. S. companies collecting personal

information latitude to operate within the more stringent European Union's privacy protections. Under these safe harbor principles, U. S. organizations may voluntarily comply with the safe harbor. Methods for compliance include joining a self-regulatory program that adheres to safe harbor principles; developing a privacy policy that adheres to safe harbor principles; or be subject to a statutory, regulatory, administrative or other body of law that effects personal privacy.¹ Companies must self certify with the Federal Trade Commission annually and publicly declare their compliance with the safe harbor provisions. Notice of compliance must be posted in the online privacy notice required for most companies that collect identifiable personal information via their web site. The Department of Commerce will maintain a regularly updated, public list of complying entities, and the list will available online at www.ita.gov/ecom after November 1, 2000.

Organizations must adhere to the seven principles stated in the safe harbor to fall into compliance with European privacy standards. Organizations must: (1) provide notice of its policies, information it has gathered, and the use made of such information; (2) allow consumers to opt out; (3) describe any transfer(s) to third parties; (4) allow access to personal information; (5) provide adequate security measures to protect information; (6) maintain the integrity of the information, and (7) provide adequate enforcement mechanisms. Failure to abide by any principle will result in removal from the safe harbor list.

As an enforcement mechanism, organizations will be required to develop and implement a dispute resolution system that allows for and resolves individual complaints. In addition, procedures for verifying compliance with the safe harbor provisions must also be developed. The procedures must be buttressed by sanctions severe enough to ensure compliance. As part of the sanctions, violations must be publicized and, in certain circumstances, data may be deleted. Sanctions may also include removal from the safe harbor program, by virtue of suspension from membership in a privacy program. In the event of non-compliance, organizations may be subject to federal or state action for deceptive trade practices, in addition to expulsion from a privacy consortium.

5. Federal Electronic Signature Law (E-Sign)

On June 30, 2000, President Clinton signed into law House Bill 1714, the Electronic Signatures in Global and National Commerce Act. The E-Sign Act will be effective October 1, 2000.

The Act allows an authorized, electronic signature to complete a commercial transaction via the Internet or any other electronic means. In addition to validating electronic transactions, the Act also allows consumers to be notified electronically if they consent to electronic delivery and can demonstrate that the information can be accessed in electronic form. The new law equates electronic drafts of contracts or agreements

¹ <http://www.ita.doc.gov/td/ecom/SafeHarborOverviewAug00.htm>

affecting commerce with their more traditional written counterparts. In most cases, the courts will honor agreements containing electronic signatures, unless the authenticity of a signature can be successfully challenged.

The parties engaged in electronic commerce that requires execution of agreements may negotiate their own solution and terms for verifying and employing the use of electronic signatures. The law itself merely authorizes the use of electronic signatures without proscribing how they should be obtained or the types of technologies used to obtain the signature. The Act does not mandate the use of electronic signatures, and parties may freely choose whether they will employ such methods. In the event that parties choose to use electronic signatures, they should include an explicit statement of the use of electronic methods and the processes for verifying and maintaining secure transactions within their agreement.

The Act applies only to commercial transactions. Will and trusts are excluded, as are family law matters like custody orders. In addition, Section 103 specifically excludes transactions that are regulated by a Federal Agency that uses a uniform standard for data sharing. Under this exclusion, HIPPA or other similar regulations appear to be unaffected by the passage of the Act. States may preempt the Act only by adopting the Uniform Electronic Transactions Act or by passing a law that is technologically neutral. Securities transactions are also covered by the Act.

In essence, the Act places electronic transactions within the statute of frauds and creates an open marketplace for electronic signature technologies by not specifying a universally required technology.

E. CONCLUSION

In many ways, the tasks and approaches associated with successfully implementing HIPAA administrative simplification requirements are (for better or worse) reminiscent of the Y2K effort. January 1, 2000 has come and gone with only isolated incidents of problems. Although some would argue that the potential Y2K problems had been overstated, there appears to be little doubt that concerted and organized effort to identify and remedy potential Y2K problems played a large part in avoiding more serious issues at the turn of the century. It is hoped that some of the lessons learned during Y2K efforts will be helpful in addressing HIPAA and related challenges.

Why does the required HIPAA effort appear similar to the Y2K effort? Similarities include:

- A firm and fixed deadline (although HIPAA's deadlines are imposed by law, and may be subject to political pressure and change)
- A technically complex subject that requires examination of business policies and procedures throughout the organization

- Potentially serious legal ramifications for failure to comply
- The need for coordination between information technology, senior management, and other units within the healthcare organization.
- No shortage of vendors and consultants scrambling to help you with the effort!

This Section introduces some steps that can be taken now in preparation for implementation of HIPAA to reduce the risks arising from or involving the disclosure of electronic patient records.

1. Update Security and Privacy Measures and Policies

As noted above, the effect of the HIPAA rules and the privacy and data protection issue on health care organizations, no matter how the final rules end up, will be very large.

Organizations must begin now to upgrade both their technology (especially security systems) and policies (including use of technology, password usage and management, contracting policies, etc.) in an effective way. Improvements in these areas should help minimize legal risks associated with unauthorized access to medical information, no matter the eventual details found in final HIPAA rules.

In addition, companies should seriously consider appointing an organizational “point person” or committee to see privacy, security and related policy upgrades to completion.

Organizations should learn from the successes (and failures) of their Y2K effort and establish a similar structure to deal with the privacy issue in their organization. The initial steps for such a privacy task force will be to: (1) conduct an inventory of privacy and security issues; (2) establish a plan to address needed technology and policy improvements; and (3) begin conducting education and awareness projects. The task force should include representatives from the information systems, health care, legal, marketing and senior management divisions of the organization.

Health care institutions need to begin updating security and confidentiality policies and systems now in order to be compliant with substantial rules and regulations that will be effective in only two (2) years.

2. Seek Contractual Privacy and Data Security Commitments

Given the importance and profile of the privacy issue, companies should seek specific privacy and data use commitments in any transaction that may touch on health information of any kind, including both new contracts and renewals of existing contracts.

Some or all of the HIPAA business partner provisions can be negotiated and inserted in contracts with vendors today. To facilitate standard transactions and purchases, privacy

and data use statements should be added to standard purchase order forms, and health care information system vendors should consider adding privacy provisions to their standard agreements as well.

Many consulting and technology service companies will offer assistance to companies in addressing Year 2000 problems. Contracts for such services generally should include provisions that:

- Document the types of services the independent contractor will provide (independent review and audit, inventory assessment, system updating, third-party vendor management);
- Specify the procedures that will be followed in auditing and modifying a company's systems;
- Determine the scope of the covenants and warranties the contractor shall provide;
- Obtain assurances that the contractor will not infringe intellectual property laws, and allocate intellectual property rights in modified code to the purchasing company (typically, without a written agreement to the contrary, the contractor developer will own modifications and new software, even if funded by the purchasing business).

3. Insurance

The health care organization should review its current insurance coverage to determine if and to what extent it would be protected in the event of a disclosure of patient information, and should investigate the availability of additional or different insurance that might provide additional coverage. Many insurance companies have recently begun offering coverage for web site and e-commerce liabilities, and these and other options should be investigated.

4. Mergers and Acquisitions

Companies involved in merger and acquisition transactions should be very sensitive to the privacy issue. The buyer should perform careful due diligence of the seller's privacy and data use policies and practices to see if there will be any legal or public relations ramifications from merging of databases containing personal information.

5. Respect Other's Intellectual Property

As part of the HIPAA implementation project, companies will probably review and test software owned by software vendors and licensed to the user company. Most license agreements contain provisions which bar the licensee from discovering the source code for the software or allowing third parties access to the software, which is often treated as the vendor's trade secret. Unauthorized copying of the software may constitute not only a breach of contract, but also infringement of the copyright or patent in the software and misappropriation of trade secrets. Companies, especially those using a services provider or other contractors for assessment and modification services, may need to contact software vendors and obtain permissions to provide access to and make modifications to licensed software.