HIPAA Update

An Advisory from the HIPAA Practice Group at Wiggin & Dana

April 2003

HIPAA Practice Group

Jeanette C. Schreiber, Chair
203.498.4334
jschreiber@wiggin.com

Maureen Weaver
203.498.4384
mweaver@wiggin.com

Michelle Wilcox DeBarge
860.297.3702
mdebarge@wiggin.com

Catherine P. Baatz
860.297.3748
cbaatz@wiggin.com

Mark W. Heaphy
203.498.4356
mheaphy@wiggin.com

Stacie Kelly
203.498.4369
skelly@wiggin.com

Amanda Littell
203.498.4529
alittell@wiggin.com

Jennifer N. Willcox
203.498.4396
jwillcox@wiggin.com

Wiggin & Dana LLP
Counsellors at Law

New Haven
Hartford
Stamford
Philadelphia
Cherry Hill

www.wiggin.com
www.HIPAA-law.info
www.healthIT.info

www.HIPAAPassport.com

April 2003 has arrived and with it key milestones on each HIPAA front. This update addresses the status of each major HIPAA component, including the recently adopted final Security Rule.

A. Final Privacy Compliance: Still a Few Loose Ends

On April 14, we will celebrate with many of you the near completion of many months of hard work in setting the HIPAA privacy compliance framework; coordinating the effort; developing numerous policies, procedures, forms, and documentation; contacting all those business associates and training the workforce. As these efforts begin to wind down, please keep in mind the following:

Document your compliance efforts. Even if a problematic incident or other noncompliance event occurs, documentation of a comprehensive implementation effort and compliance structure will be very helpful in demonstrating your responsible good faith efforts.

Use care to avoid creating additional obligations. Whether you have adopted a "boilerplate" set of policies or have carefully drafted your own, remember that language used in your policies and procedures may unintentionally result in additional obligations beyond HIPAA which can create legal responsibilities. Be sure to continue to review your new policies and procedures to assure they do not unnecessarily create new requirements that go even beyond HIPAA.

Be alert for further interpretations and guidance. Evolving interpretations will come from the Office for Civil Rights (OCR) and industry sources as implementation issues and questions surface. These may lead to some fine-tuning of your new policies and procedures. Provide updates to staff as needed, and remember to update your compliance documentation.

Consider your compliance as a Business Associate. Many health care providers and health plans have affiliates or divisions that are not HIPAA covered entities but serve as business associates to the covered entity or to others. Several state agencies will be issuing business associate agreements to programs that receive state funding. Most of the HIPAA privacy requirements for covered entities also apply to business associates because of the required language in the business associate agreements (such as restrictions on uses and disclosures, minimum necessary, use of authorizations, tracking and accounting for disclosures, etc.) It may be necessary to expand your privacy compliance efforts and structures to include related business associates. Also, remember that subcontractors of business associates also must sign agreements containing similar business associate language.

Keep an eye on your state law. Implementation of HIPAA has shined a spotlight on state privacy laws. If you used "boilerplate" policies that did not address the laws of each state in which you

operate, give careful consideration to any state law implications that may impact your operations. Also, remember that like HIPAA, state law, regulations and interpretation will be evolving. Be alert to changes and be proactive in addressing questions or concerns.

Build HIPAA compliance into your organization's overall compliance program. A final step in HIPAA privacy implementation should be building a program of self-audits and other compliance monitoring into your overall corporate compliance structure. Assure that ongoing responsibilities are maintained and documented including ongoing training and education; updating the Privacy Notice, forms and policies when needed; documenting HIPAA-related activities; handling complaints and incidents in coordination with risk-management; and imposing sanctions and disciplinary action when necessary to enforce privacy requirements.

Congratulations on making it to April 14, 2003! Even though you undoubtedly still have at least a few tasks left on your HIPAA privacy list, you are on your way to integrating these new requirements into your operations.

B. Transactions and Code Sets (EDI) Regulations: Let the Testing Begin

When Congress authorized the compliance deadline extension for the Transactions and Code Sets (EDI or electronic data interchange) regulations, it required covered entities submitting compliance plans to qualify for the extension to commit to begin testing these new transactions by April 16, 2003. The EDI HIPAA rules govern the electronic transmission by covered health plans, providers and clearinghouses of claims and related transactions specified in the regulations. Whether you are handling this part of HIPAA compliance in-house or through a vendor, it is important to document readiness for testing by April 16.

The final compliance date for the EDI HIPAA requirements was originally October 16, 2002 (small health plans until October 16, 2003), but was extended to October 16, 2003 for covered entities that filed a compliance plan with the Centers for Medicare and Medicaid Services (CMS). Covered entities whose billing companies or software vendors are unable to provide assurances of timely compliance with the HIPAA EDI requirements should find new vendors.

On February 20, 2003, CMS published some final modifications to the EDI regulations. These changes removed the National Drug Codes as the standard code set for drugs and biologicals in non-retail pharmacy transactions and adopted some technical changes to the implementation standards.

You may receive requests to sign Trading Partner Agreements (TPAs) in connection with EDI compliance. Although these agreements are mentioned in the HIPAA EDI regulations, they are not required. Since the purpose of TPAs is solely to address technical aspects of the EDI transmission, use care in reviewing any draft TPA for any extraneous or problematic requirements so as to avoid undertaking any additional legal responsibilities not required by HIPAA. Recently Wiggin & Dana HIPAA lawyers worked closely with the Connecticut Department of Social Services (DSS) to assure a final DSS TPA that fairly addresses the relevant issues. (DSS has agreed that any Connecticut Title XIX providers that signed the earlier TPA may substitute the revised edition.)

C. Final Security Rule: The Next Wave

On February 20, 2003, the Department of Health and Human Services, Centers for Medicare and Medicaid Services (CMS), published the final HIPAA security standards, Health Insurance Reform: Security Standards; Final Rule, 45 CFR Parts 160, 162 and 164, 68 Fed. Reg. 8333 (Feb. 20, 2003). These standards establish a security management framework for protection of Electronic Protected Health Information (EPHI). Significantly, the final HIPAA Security Rule applies only to protected health information in electronic form and, unlike the Privacy Rule, does not cover physical documents or oral information. CMS continued to defer indefinitely standards for electronic signatures.

The final compliance date for the Security Rule is April 20, 2005. Thus, final efforts to meet the April 14, 2003 Privacy Rule compliance date and to begin testing under the Transactions and Code Sets Standards by April 16, 2003 will continue to have priority.

The final Security Rule was drafted to be very compatible with the Privacy Rule and these provisions share common definitions and compliance structures. For example,

"Affiliated Covered Entities" under the Privacy Rule can be expanded to include security compliance. The Privacy Rule requirements to use reasonable administrative, physical and technical safeguards will eventually be informed and amplified for EPHI by the organization's security compliance.

General Rule

Generally, the Security Rule requires a covered entity to:

> 1) Ensure the confidentiality, integrity, and availability of EPHI that the covered entity creates, receives, maintains, or transmits;
> 2) Protect against any reasonably anticipated threats or hazards to the security or integrity of EPHI;
> 3) Protect against any reasonably anticipated uses or disclosures of EPHI that are not permitted or required; and
> 4) Ensure workforce compliance.

45 C.F.R. 164.306(a).

In keeping with the CMS commitment to "scalable" and "technology neutral" requirements, the Security Rule allows flexibility in how a covered entity chooses to meet certain requirements, considering such factors as the cost of a particular security measure, the size of the covered entity, the complexity of the approach, the technical infrastructure and other security capabilities in place, and the nature and scope of potential security risks. Rather than requiring specific technical measures, the Security Rule takes a goal-oriented approach, establishing "standards" that all covered entities must meet, accompanied by implementation specifications to guide compliance with each standard.

The implementation specifications are divided into two categories: required and addressable. Covered entities must implement all required implementation specifications, deemed fundamental to any reasonable security compliance program. For addressable implementation specifications, however, a covered entity must assess the reasonableness and appropriateness of each specification to its own security framework. It may decide to implement an alternative security measure or may determine that the particular specification is not applicable, documenting the rationale and approach taken to meeting the standard to which the implementation specification relates. As noted, in making this assessment a covered entity may consider a variety of factors, including "the entity's risk analysis, risk mitigation strategy, what security measures are already in place, and the cost of implementation." In all cases, however, the covered entity must meet the applicable standard.

Standards

The Security Rule identifies three categories of standards: administrative, physical and technical.

Administrative safeguards primarily address the policies and procedures a covered entity must have in place to document its ability to insure the confidentiality, integrity and availability of EPHI. There are nine administrative security standards, including Security Management Process, Assigned Security Responsibility, Workforce Security, Information Access Management, Security Awareness and Training, Security Incident Procedures, Contingency Plan, Evaluation, and Business Associate Contracts and Other Arrangements. To meet these standards, a covered entity must implement required implementation specifications, such as Risk Analysis, Risk Management, Information System Activity Review, Response and Reporting, Data Backup, Disaster Recovery, and Emergency Mode Operation. There are also important addressable implementation specifications, such as Authorization and/or Supervision, Workforce Clearance Procedures, Termination Procedures, Access Authorization, Protection from Malicious Software, and Password Management.

Physical safeguards focus on the physical security measures in place to secure EPHI. The applicable standards are Facility Access Controls, Workstation Use, Workstation Security, and Device and Media Controls. The required implementation specifications include, for example, Disposal and Media Re-use, and the addressable implementation specifications include Contingency Operations, Facility Security Plan, Access Control and Validation Procedures, Maintenance Records, Accountability, and Data Backup and Storage.

Technical safeguards detail the standards for access control, auditing, user authentication and other technical measures involved in securing stored and transmitted EPHI. Technical

The Wiggin & Dana HIPAA PRACTICE GROUP ADVISORY is a periodic newsletter designed to inform clients and others about recent developments in the field of HIPAA law. Nothing in the HIPAA PRACTICE GROUP ADVISORY constitutes legal advice, which can only be obtained as a result of personal consultation with an attorney. The information published here is believed to be accurate at the time of publication, but is subject to change and does not purport to be a complete statement of all relevant issues. If you have any requests for topics or other suggestions, please contact Advisory editor Jeanette C. Schreiber 203.498.4334, jschreiber@wiggin.com.

safeguards include five standards, which are Access Controls, Audit Controls, Integrity, Person or Entity Authentication, and Transmission Security. The required implementation specifications include Unique User Identification and Emergency Access Procedures, and addressable implementation specifications include Automatic Logoff, Encryption and Decryption, Mechanisms to Authenticate EPHI, and Integrity Controls.

For a complete list of the Security Rule's standards and implementation specifications, please see the attached chart.

Business Associate Agreements

The Security Rule now embraces the Privacy Rule's concept of business associate agreements, requiring covered entities to enter into such contracts with business associates who create, receive, maintain or transmit EPHI on their behalf. The final Security Rule applies the same definition of "business associate" as the Privacy Rule, and eliminated the proposed separate "chain of trust" agreement provision. Under the Security Rule, a business associate must:

- implement administrative, physical and technical safeguards that reasonably and appropriately
- protect the confidentiality, integrity and availability of the covered entity's electronic protected health information;
- ensure that agents and subcontractors to whom the business associate provides EPHI do the same;
- report to the covered entity any security incident of which it becomes aware and
- authorize termination if the covered entity determines that the business associate has violated a material term.

Most business associate agreements established under the Privacy Rule will need a few amendments to comply fully with the Security Rule. As under the Privacy Rule, a covered entity is not liable for violations by its business associate unless the covered entity knew that the business associate was engaged in a practice or pattern of activity that violated HIPAA and failed to take any corrective action.

Getting Started

The timing and expense of HIPAA security compliance will depend on the nature of the covered entity and the status of its current IT/IS systems. Some larger entities may already have many of the required protections in place, while others will not. Information Systems that will be fully replaced before the April 20, 2005 compliance date must meet Privacy Rule standards but need not comply with the Security Rule unless EPHI is retained in the legacy system. All organizations will need to develop additional HIPAA policies, procedures and documentation to address security compliance. Following are some considerations in planning your next steps:

- Assign responsibility for reviewing the Security Rule and establishing an implementation approach, timeline and budget.
- Consider asking your software vendors to specify in detail how features of your system(s) address each HIPAA security standard (recognizing that stating a system is "HIPAA compliant" does not tell you enough).
- Assess whether you need outside consulting or legal assistance to help assess your security needs.
- Begin a comprehensive security audit to understand the security measures (administrative, physical and technical) currently in place.
- Assign personnel and establish a process for assessing compliance, including the performance of a risk analysis to identify vulnerabilities.
- Target issues identified by the risk analysis and begin developing a plan to address areas of risk and achieve HIPAA compliance.
- Continue to work with industry HIPAA collaborative groups to coordinate security implementation efforts and define industry "best practices."

D. What Regulations Are Coming Next?

The next set of HIPAA regulations anticipated is the HIPAA Enforcement Rule to be developed jointly by OCR (for privacy) and CMS (for EDI and security). CMS recently announced in the Federal Register that it is establishing an Office of HIPAA to develop and update regulations and carry out CMS HIPAA enforcement.

Wiggin & Dana's Health Care Information Technology Practice Group blends world-class, health care regulatory experience with a sophisticated IT practice to provide sound, practical counsel regarding health care-related information technology, legal and business issues. Our practice takes into account each client's operational needs, goals, and priorities, and applicable state and federal regulatory requirements.

We serve a diverse group of health care IT clients: health care providers, systems, and networks, health care provider associations, and health plans; and e-commerce businesses, software developers, data clearinghouses and networks, web designers, IT vendors, suppliers, consultants, and application service providers to the health care industry.

Our lawyers are well versed in the technical, regulatory, business, and practical considerations shaping IT in the health care world. We help clients manage the business risks and legal issues associated with health care-related IT systems and services, including the electronic exchange of health information and data, e-commerce, and intranet and Internet activities. Our lawyers:

- Develop policies, procedures, notices, contracts, and other documentation required under HIPAA (the Health Insurance Portability and Accountability Act of 1996) as well as other federal and state laws regarding security, privacy, and other government requirements for health information management;
- Advise clients concerning the computerization of medical records and health claims information, the collection and electronic transmission of confidential patient information, the delivery of Internet-based health services, and other health care e-commerce;
- Negotiate complex outsourcing arrangements for administrative and IT functions;
- Assist in the creation and operation of electronic databases and repositories;
- Help structure Internet-based services and assist with e-commerce ventures and other entrees into the digital world;
- Draft, review, and negotiate software development and licensing contracts;
- Advise clients on the digitization of medical imaging, and the development of telemedicine;
- Audit processes, contractual arrangements, services, and products for compliance with federal and state requirements;
- Provide ongoing advice concerning health information technology issues by keeping abreast of legislative and regulatory changes and industry developments;
- Prepare written testimony and work on strategic efforts relating to legislative and regulatory issues, proposals, and changes affecting our clients; and
- Provide in-service and other educational information and programs for our clients' staff, consultants, vendors, and customers.

HIPAAPassport ™

Developed by Wiggin & Dana LLP in collaboration with Simione Constants, LLC, this three CD series is designed to help you fast track your HIPAA implementation. After the HIPAA compliance dates, the CDs will serve as a valuable resource on each of the Privacy and Security requirements and will provide tools for evaluating compliance. The CDs are divided into manageable "Project Guides" on Privacy and Security Rule topics. Each Project Guide contains a "plain English" summary of the requirements, model forms and policies, and various implementation tools. There is a full section on Workforce training with a ready-made slide show. The third CD, which reflects the final Security Rule provisions will be available in early summer. *HIPAAPassport* was specifically designed for home care, hospice and long-term care providers and is also being used by a wide variety of health care providers including hospitals, ambulatory surgical facilities and social service agencies. *HIPAAPassport* is recommended by the American Association of Homes and Services for the Aging (AAHSA) and by the National Association of Home Care (NAHC); a special discount is available for AAHSA and NAHC members. To order or to find out more visit www.hipaapassport.com or call 1-800-653-4043.

A Summary List of HIPAA Security Standards

Administrative Safeguards

Standards	Sections	Implementation Specifications (R) = Required, (A) = Addressable	
Security Management Process	164.308(a)(1)	Risk Analysis	(R)
		Risk Management	(R)
		Sanctions Policy	(R)
		Information System Activity Review	(R)
Assigned Security Responsibility	164.308(a)(2)		(R)
Workforce Security	164.308(a)(3)	Authorization and/or Supervision	(A)
		Workforce Clearance Procedure	(A)
		Termination Procedures	(A)
Information Access Management	164.308(a)(4)	Isolating Health Care Clearinghouse Function	(R)
		Access Authorization	(A)
		Access Establishment and Modification	(A)
Security Awareness and Training	164.308(a)(5)	Security Reminders	(A)
		Protection from Malicious Software	(A)
		Log-in Monitoring	(A)
		Password Management	(A)
Security Incident Procedures	164.308(a)(6)	Response and Reporting	(R)
Contingency Plan	164.308(a)(7)	Data Backup Plan	(R)
		Disaster Recovery Plan	(R)
		Emergency Mode Operation Plan	(R)
		Testing and Revision Procedure	(A)
		Applications and Data Criticality Analysis	(A)
Evaluation	164.308(a)(8)		(R)
Business Associate Contracts and Other Arrangements	164.308(b)(1)	Written Contract or Other Arrangement	(R)

Physical Safeguards

Standards	Sections	Implementation Specifications (R) = Required, (A) = Addressable	
Facility Access Controls	164.310(a)(1)	Contingency Operations	(A)
		Facility Security Plan	(A)
		Access Control and Validation Procedures	(A)
		Maintenance Records	(A)
Workstation Use	164.310(b)		(R)
Workstation Security	164.310(c)		(R)
Device and Media Controls	164.310(d)(1)	Disposal	(R)
		Media Re-use	(R)
		Accountability	(A)
		Data Backup and Storage	(A)

Technical Safeguards

Standards	Sections	Implementation Specifications (R) = Required, (A) = Addressable	
Access Control	164.312(a)(1)	Unique User Identification	(R)
		Emergency Access Procedure	(R)
		Automatic Logoff	(A)
		Encryption and Decryption	(A)
Audit Controls	164.312(b)		(R)
Integrity	164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information	(A)
Person or Entity Authentication	164.312(d)		(R)
Transmission Security	164.312(e)(1)	Integrity Controls	(A)
		Encryption	(A)