



HIPAA Update

April 2003

Compliance Dates and Deadlines for HIPAA Compliance

| Section | Final Rule Published | Compliance Deadline | Status |
|---|--------------------------------|---|--|
| <u>Standards for Privacy</u> | 12/28/00 | 4/14/03 ; 4/14/04 for small health plans | Modifications finalized 8/14/02; Guidance issued 7/6/01 & 12/4/02. |
| <u>Electronic Transactions and Code Sets</u> | 8/17/00 | 10/16/03 for all small health plans and covered entities that submitted an application for extension prior to 10/16/02; 4/16/03 is the deadline for covered entities to begin transaction testing | Modifications to original rule finalized 2/20/03. |
| <u>Unique Identifier for Employers</u> | 5/31/02 | 7/30/04 ; 8/1/05 for small health plans | |
| <u>Standards for Security</u> | 2/20/03 | 4/21/05 ; 4/21/06 for small health plans | Final rule consistent with privacy standards. |
| <u>Unique Health Care Provider Identifier</u> | Proposed rule published 5/7/98 | N/A | Final rule expected Spring 2003. |
| <u>Unique Health Plan (Payer) Identifier</u> | In development stage | N/A | Proposed rule expected Spring 2003. |
| <u>Standard for Claims Attachments</u> | In development stage | N/A | Proposed rule expected Spring 2003. |



Enforcement

The Office for Civil Rights (OCR) has been charged with the responsibility of coordinating enforcement efforts related to compliance with HIPAA's Privacy Rule. Efforts to implement enforcement strategies are already underway as the deadline for privacy compliance approaches. All covered entities, aside from small health plans, are required to be compliant with the privacy regulations by 4/14/03. Initially, the enforcement process will be complaint-driven. Technical assistance will be offered to covered entities under investigation to help with compliance efforts and the development of corrective action plans. The Centers for Medicare & Medicaid Services (CMS) will be responsible for enforcement of HIPAA's other Administrative Simplification rules and regulations. Penalties for non-compliance include monetary fines as well as possible jail time for offenders. See below for information on complaint submissions:

Submission of Complaints for Privacy Violations

(Published in the Federal Register March 20, 2003)

For covered entities located in New Jersey, New York, Puerto Rico, or the Virgin Islands submit complaints to:

The Office for Civil Rights

US Department of Health and Human Services

Jacob Javits Federal Building

26 Federal Plaza, Suite 3312

New York, NY 10278

Voice Phone – 212-264-3313, Fax – 212-264-3039, TDD – 212-264-2355

For address information on covered entities in other regions of the country, visit: <http://www.hhs.gov/ocr/hipaahealth.txt>.

Submission of Complaints for Electronic Transactions and Code Set Violations

Written complaint forms can be found at: <http://cms.hhs.gov/hipaa/hipaa2/support/correspondence/complaint/complaintform.pdf> and should be submitted to: HIPAA Complaint

7500 Security Boulevard, C5-24-04

Baltimore, MD 21244

Electronic complaint submissions can be filed at: <http://cms.hhs.gov/hipaa/hipaa2/support/correspondence/complaint/securitychoice.asp>.

Copyright MedComp Alliance, LLC

Not for duplication or distribution without prior written consent

Disclaimer: The information contained in this document is for educational purposes only. Please be advised that the author is NOT rendering legal advice.

Privacy Guidance – issued December 12/4/02



In December of 2002, The Office for Civil Rights (OCR) released a guidance document to dispel some of the confusion with regard to meeting the requirements of the privacy regulations. Practical answers to common questions were provided in an effort to help covered entities understand and appropriately implement the regulations. Topics covered by the guidance include Incidental Uses & Disclosures, Minimum Necessary, Personal Representatives, Business Associates, Uses & Disclosures for Treatment, Payment, and Health Care Operations, Marketing, Public Health, Research, Notice, and Government Access. The guidance can be found in its entirety at <http://www.hhs.gov/ocr/hipaa/privacy.html>.

Highlights of the document are summarized below:

Incidental Uses & Disclosures – Health care providers are allowed to engage in confidential conversations with other providers or with patients even if there is a possibility that they could be overheard, as long as the minimum necessary standard is followed and reasonable precautions are taken to minimize the chance of an incidental disclosure from happening. There is no need to document the occurrence of incidental disclosures. HIPAA's Privacy Rule does not require structural changes in the facilities of covered entities. However, reasonable safeguards to limit incidental disclosures and prevent prohibited disclosures must be implemented.

Minimum Necessary – The minimum necessary standard is not an absolute standard, thus requiring covered entities to use professional judgment to determine the appropriate amount of information to be disclosed in various situations. Disclosures for treatment purposes are excluded from the minimum necessary standard.

Personal Representatives – In general, the Privacy Rule grants those individuals with rights to make health care decisions for an individual, the ability to exercise the rights of that individual with respect to health information. The granting of Power of Attorney privileges for purposes other than health care, such as for real estate, does not allow that person to have access to the individual's protected health information (PHI).

Business Associates – Written contracts between covered entities and their business associates are required when PHI is disclosed to the business associate so that the business associate can perform a function on behalf of the covered entity. Covered entities are not required to monitor the actions of their business associates. However, all business associate contracts must contain a clause that allows covered entities to terminate a contract should the business associate commit a breach of privacy. Business associate contracts are not required when information is shared between health care providers for treatment purposes. Business associate contracts are not required for those individuals that may have inadvertent contact with a covered entities' PHI. An example would be the janitorial services contracted to clean the office after hours. Additionally, organizations such as the US Postal Service are considered conduits of information and do not require business associate contracts.

Uses and Disclosures for Treatment, Payment, and Health Care Operations – HIPAA does not affect informed consent for treatment, which is addressed by New York State law. Health care providers are not required to obtain patient authorization to consult with another provider for treatment purposes.

Privacy Guidance Continued

Marketing – Authorization is required before a covered entity can use or disclose PHI to engage in marketing activities. The exceptions to the authorization requirement are (1) face to face communications between the covered entity and the individual and (2) communication involving a promotional gift of nominal value. If the covered entity will receive direct or indirect remuneration from a third party for a marketing activity requiring authorization, the authorization must state that remuneration is involved.

Disclosures for Public Health Activities – A covered entity does not need to obtain permission from a patient prior to notifying public health authorities of the occurrence of a reportable disease.

Research – Authorizations obtained for research purposes may state that the authorization does not expire or expires at the end of the research study. Authorizations may be combined with consents to participate in the research, or with any other legal permission related to the research study.

Notice of Privacy Practices – When the first treatment encounter, after April 14, 2003, is not face to face, the covered entity should send their Notice of Privacy Practices, along with some type of acknowledgement to return, to the patient as soon as possible.

Government Access – HIPAA does not expand current law enforcement access to PHI. The Privacy Rule does not create a government database with all individuals' PHI.

10 Things Your Privacy Officer Should Consider as the Deadline for Privacy Approaches



1. Is there a **written description** of the Privacy Officer's **responsibilities** on file?
2. Has the **Notice of Privacy Practices** been finalized? Has it been posted or are there plans to do so before April 14, 2003? Has a system to obtain written acknowledgement of the Notice by patients been established?
3. Is a system in place for dealing with **complaints** that are presented to your organization?
4. Are your **privacy policies** in place?
5. Has your **workforce** received **training**? Is there record of this?
6. Have all members of your workforce signed **confidentiality agreements**?
7. Have **business associates** been identified and contracts put in place as necessary?
8. Are **minimum necessary** standards in place?
9. Is the **fax machine** in a **secured** area? Are **cover sheets** being used for all faxes containing PHI?
10. Are **authorization forms** finalized and ready for utilization?

Final Security Rule Published 2/20/03

The final HIPAA Security Rule was published on February 20, 2003. This long awaited final rule has achieved greater synchronicity with the Privacy Rule with the addition of similar terms and definitions. The final Security Rule is consistent with the proposed version in its commitment to requiring covered entities to develop, implement, and maintain high standards for security of PHI. Most covered entities will be required to be compliant with the Security Rule on April 21, 2005.

The security regulations call for the protection of electronic PHI, but reference to particular technologies is excluded. This was deliberate in an attempt to facilitate the implementation of the standards. The regulations will require health care providers to implement the following:

- Administrative Safeguards – identification and implementation of appropriate security measures
- Physical Safeguards – protection of electronic PHI against environmental factors and unauthorized access
- Technical Safeguards – mechanized means to protect electronic PHI
- Organization Requirements – standards related to business associate agreements or other arrangements
- Policies and Procedures – implementation of reasonable and appropriate policies and procedures to comply with the standards

Similar to the privacy regulations, the security regulations have been written so that they can be scaled to the particulars of an organization. The final rule has separated standards from implementation specifications in an effort to assist with compliance efforts. The standards are the essential components of the regulations and describe the deliverables of implementation. The implementation specifications, which guide the implementation of the standards have been labeled “R” for required or “A” for addressable. Required specifications must be implemented prior to the April 21, 2005 deadline. Addressable specifications must be considered in the implementation process, and if deemed necessary and appropriate, implemented by April 21, 2005.

To view the Security Rule in its entirety go to:

<http://cms.hhs.gov/hipaa/hipaa2/regulations/security/default.asp#finalrule>.



CMS Website

The Centers for Medicare & Medicaid Services (CMS) has devoted a section of their website to HIPAA related issues. You can visit the site at <http://cms.hhs.gov/hipaa/hipaa2/default.asp> to access general information on HIPAA, read the full text versions of the regulations, obtain information on enforcement, upcoming events, and education materials, and electronically submit complaints for electronic transactions and code sets violations.

Other HIPAA Websites

<http://www.oft.state.ny.us/hipaa/> - New York State Office for Technology

<http://www.hhs.gov/ocr/hipaa/privacy.html> - Office for Civil Rights

<http://www.massmed.org/pages/hipaaguidebook.asp> - Massachusetts Medical Society

http://library.ahima.org/xpedio/groups/public/documents/web_assets/bok1_016846.hcst - AHIMA