



HIPAA Update

October 2003

Copyright 2003 - 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.



HIPAA Privacy has Arrived!

The date for compliance with HIPAA's Privacy Rule has come and gone, but have the objectives of the rule truly been met? Are all covered entities fully compliant? According to a HIMSS/Phoenix Health Systems survey earlier this year, the answer is no. The survey results indicate that most of the highly publicized requirements, (ie. privacy notice, authorization forms, etc.) have been met, but that more complex issues, like the business associate requirements, have not been tackled by all covered entities. Additional details of the survey can be found at www.hipaadvisory.com.

So what does this mean? Are the HIPAA privacy police ready to begin investigating the thousands of potential violators out there? All indications suggest not. During this first year, enforcement of the Privacy Rule is expected to be complaint driven and allow for corrective action plans to be established and implemented prior to imposition of penalties.

Beyond the Basics with Privacy

Monitoring for Compliance with the Privacy Rule

As time goes by, a clearer picture of the level of compliance and enforcement within the industry will emerge. For now, continued efforts to maintain and monitor compliance with the rule are recommended. These activities can include:

- Using stickers to recognize compliant and non-compliant behavior. Generic stickers can be purchased or custom stickers can be created in-house or purchased for a relatively small expense. Privacy Officers can perform spot checks of employee work areas. Leave stickers, on the desks of employees, expressing appreciation for compliance when there is evidence that your privacy policies have been followed. Leave a sticker too, if there is evidence of non-compliant behavior. This sticker should serve as a warning. A note describing the violation might also be left on the employee's desk.
- The distribution of periodic tips related to ongoing HIPAA compliance via e-mail. Reminding employees that the company has not forgotten about HIPAA will set the tone for continued compliant behavior.
- The monitoring of desks, trash cans, and other areas within the facility to see if documents containing protected health information (PHI) have been appropriately put away or disposed of at the end of each day. Monitoring in this manner is cost-effective.
- Displaying posters throughout the facility to promote HIPAA awareness. Posters can be purchased, but an employer might also want to sponsor a poster making contest for employees.
- Creation of a HIPAA incentive program for the entire company to work towards. Companies whose employees are required to drive significant amounts of miles are often rewarded after a certain number of accident free miles. Why not do something similar? For each month that no HIPAA violations are reported to or identified by the Privacy Officer, provide a pizza party for employees.
- The delivery of periodic refresher training classes. On a yearly basis, reorient employees to the fundamentals of HIPAA. An employer might also want to consider dedicating time to HIPAA in already scheduled staff meetings.
- Having the Privacy Officer pose as a patient or other individual trying to get information that would not be allowed by HIPAA in an effort to truly test employees' understanding of, and compliance with, the boundaries set by this legislation.
- Making a diligent effort to apprise employees when changes to the regulations take effect and also when changes to internal policies and procedures are implemented. It is all too often that the last to know about changes are ones most affected.

Sharing of PHI for Treatment Purposes

Copyright 2003 - 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.

Providers are sometimes confused about the conditions for sharing information for treatment purposes. Providers can still confer about the treatment of a patient with another provider without authorization or consent from the patient. Providers can continue to carry on conversations in semi-private areas as long as reasonable protections to prevent or limit wrongful disclosure of PHI have been implemented. In the case of an emergency room where curtains separate patients, a lowered voice would be a good precaution to take to limit the amount of information other patients could overhear.

Notice of Privacy Practices

The Notice of Privacy Practices has also raised questions among providers. There are several things to consider once your Notice is finalized. Make sure you are distributing it to all patients the first time they present for service after April 14, 2003. Attempt to obtain a written acknowledgement of receipt on that first visit too. Post the Notice prominently in your office and on your website, if you maintain one.

Communication Media

Another area that seems to have received great attention is that of communication. Are telephones and cell phones prohibited? What about fax machines? The answer is no, none of these items have been banned by the HIPAA Privacy Rule. However, reasonable precautions must be implemented to limit and/or prevent inappropriate disclosures of PHI. For example, messages can be left on answering machines, but a minimum amount of information should be left. 'Mrs. Jones, please call 333-4444 regarding your appointment' would be appropriate, but 'Mrs. Jones, the results of your pregnancy test are in so please call Dr. Sedgewick's Office immediately at 333-4444' would not.

Business Associate Contracts

A 'business associate' is defined as an entity that a covered entity shares PHI with to carry out a function on their behalf. Contracts, or amendments to existing contracts, are required to ensure protection of information shared between these two types of entities. Common examples include billing companies, transcription services, and document destruction vendors. For all new contracts after October 15, 2002, the provisions should have been in place by April 14, 2003. Contracts that were in place prior to October 15, 2002, have up to an additional year to comply. Provisions are required on the contract renewal date or by April 14, 2004, whichever comes first. The required elements in a contract to meet the business associate provisions can be found at <http://www.hhs.gov/ocr/hipaa/contractprov.html>. Legal counsel should be contacted when appropriate.

Accounting for Disclosures

The accounting for disclosures provision in the Privacy Rule requires covered entities to maintain a record of all disclosures of PHI that are not for treatment, payment, healthcare operations or allowed by authorization. Patients have a right to receive a copy of all such disclosures. Examples include releases to health oversight agencies and communicable disease reporting as required by law. It is also recommended that accidental disclosures also be included. An example would be misdirected faxes.

Managing this requirement takes a cooperative effort by all those involved. First, establish a documentation system, then present it to employees, giving them the chance to make suggestions for improvement and to get a clear understanding of your expectations. The system can be a simple form that is completed and placed in patient charts or you can keep a log of all disclosures. The key to compliance is being able to easily produce all such disclosures when a patient asks for an accounting.

Authorizations

Authorization forms, with specific elements are required for PHI to be shared for purposes other than for treatment, payment, healthcare operations, or as required by law. The required elements for an authorization form can be found at <http://www.hipaadvisory.com/regs/finalprivacy/508.htm>.

HIPAA compliant authorization forms are **generally needed** in the following situations:

- To disclose PHI about a patient to a third party (i.e., a life insurance underwriter);
- To market a product or service;
- To raise funds for any entity other than your practice;
- For research unless your practice has a signed waiver approved by the Institutional Review Board (IRB) for the use and disclosure of PHI or has de-identified PHI;

HIPAA compliant authorizations are generally **NOT needed** in the following situations:

- To a provider who has a direct treatment relationship with the patient
- To a health oversight agency with respect to audits, civil, administrative, and/or criminal investigations, proceedings or actions, inspections, licensure or disciplinary actions
- In response to a court order, court-ordered warrant, subpoena or summons
- To law enforcement for the purpose of identifying or locating a suspect, fugitive, material witness or missing person, (e.g., disclosing a deceased individual's PHI if suspicion persists that death may have resulted from criminal conduct)
- To organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of organs, eyes or tissue for donation and transplantation
- As required by law for public health activities and the prevention or control of disease, injury or disability, including but not limited to communicable diseases and product defects or problems (e.g., with food and dietary supplements and product labeling issues)
- As required by law to social or protective services with respect to victims of abuse, neglect or domestic violence
- Of Armed Forces personnel for activities deemed to assure proper execution of military mission
- To authorized federal officials for the conduct of lawful intelligence or counter-intelligence as authorized by the National Security Act
- To authorized federal officials as it relates to protecting the President of the United States, to foreign heads of state or other authorized persons
- To the United States Department of State as it relates to obtaining security clearance, service abroad and other provisions of the Foreign Service Act
- To correctional institutions or law enforcement as it relates to inmates' healthcare or the health and safety of individuals treating and transferring inmates
- To a person who may have been exposed to a communicable disease, if the practice is authorized by law to notify such persons in the conduct of a public health intervention or investigation
- To an employer, if the practice is a covered provider who is a member of the workforce of the employer or who provides healthcare to the patient at the request of the employer: to conduct an evaluation relating to medical surveillance of the workplace; or to evaluate whether the individual has a work-related illness or injury
- To an auto insurance company (re: No Fault Insurance Claims) or workman's compensation boards (re: on-the-job injuries) when they are responsible for payment of the practice's services

A little common sense, good professional judgment and a general understanding that HIPAA was not invented to impair the ability of physicians to provide appropriate care for patients will go a long way in the battle to achieve and maintain compliance with the Privacy Rule.

Transaction and Code Set Deadline: **Is the Industry Prepared?**

Copyright 2003 - 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.

Compliance with HIPAA's Transaction and Code Sets (TCS) Rule was originally required by October of 2002, but the passing of the Administrative Simplification Compliance Act in December 2001 allowed covered entities to apply for an additional one year to achieve compliance with these complicated and often controversial regulations. Most entities submitted the necessary documentation to receive the extension, but it remains unclear if full compliance will be achieved by the October 2003 deadline, just a few months away.

A letter to the Secretary of the Department of Health and Human Services (DHHS) [Tommy G. Thompson] dated June 25, 2003 from John Lumpkin, Chair of the National Committee on Vital and Health Statistics identifies a variety of reasons that the deadline will not be met and urges the DHHS to 'provide flexibility in enforcement during a transition period' and to 'provide additional clarification and guidance' on the details of the regulations. The letter, in its entirety can be found at <http://www.hipaadvisory.com/news/2003/0702ncvhs.htm>.

According to the regulations, payers are not allowed to accept non-compliant transactions past the October 15 deadline. For providers unable to send compliant transactions, this has the potential to cause a major disruption in cash flow. Experts recommend that covered entities have a contingency plan to offset any cash flow shortages while continuing efforts to achieve compliance.

Security Rule Update

With a deadline so far in the distance [April 2005] is it really necessary to begin looking at the security regulations? There were changes to the final Privacy Rule and changes to the final Transaction and Code Sets Rule. Will there be changes to the Security Rule?



Chances are yes, there will most likely be changes to the security regulations, but that does not mean covered entities should await these anticipated changes or additional guidance from CMS to begin their compliance efforts. Unlike the Privacy Rule, there are many requirements in the Security Rule that cannot be achieved in a single day or without a significant level of technological expertise. This being said, entities should begin to examine the regulations now, instead of waiting to the last minute, as many entities did with the Privacy Rule.

A risk analysis is the foundation for implementation of the Security Rule and must be completed long before the 2005 deadline in order to allow time for installation of the security mechanisms identified by the analysis. Covered entities should first decide if they will hire an outside source or utilize in-house resources to facilitate the implementation. Then, with these resources, begin efforts to achieve compliance.

As part of the risk analysis, covered entities are required to inventory all electronic protected health information (EPHI) within their organization and list in detail security mechanisms already in place. A comparison to the requirements of the Security Rule is then carried out, allowing covered entities to identify gaps between their current operating procedures and compliance. This may sound like, and most likely will be, an overwhelming task, which is why covered entities are urged to begin now.



Interim Enforcement Rule Published

On April 17, 2003 an Interim Enforcement Rule was published in the Federal Register to establish the guidelines for enforcement of the HIPAA Administrative Simplification rules. Published on the heels of HIPAA's privacy compliance date [April 14,2003], this rule gives the Office for Civil Rights, the entity charged with enforcement of the Privacy Rule, procedures for conducting investigations, guidelines for imposition of penalties, and rules for hearings. The enforcement efforts for HIPAA's many other requirements including the Transactions & Code Sets and Security Rules, will also be governed by this rule. Visit <http://www.cms.hhs.gov/hipaa/hipaa2/default.asp> to read the full text.

Identifier Rules

HIPAA's identifier rules have not brought about as much controversy and concern as have the Privacy and Security Rules, but are still important components in achieving the administrative simplification goals intended by HIPAA. Providers deal with a multitude of entities including health plans, payers, clearinghouses, patients, and vendors on a daily basis, each requiring a different identifying code or number. The countless identifiers that a provider is currently assigned can be a logistical nightmare. Processing delays, disruptions in cash flow and wasted man hours to research errors are just a few of the problems that continuously arise.



The intent of the Identifier Rule is to eliminate the confusion and extra work associated with this unmanageable system by standardizing transaction data elements. Providers, employers, and health plans shall be assigned and required to utilize just one identifier for all of their transactions, easing the administrative burden for everyone. The problem has been in identifying identifiers that will, with minimal reformatting or reprogramming, allow for easy transition. The benefits may not outweigh the costs if entities are required to perform extensive restructuring of their computer systems, or have to purchase new systems all together.

With the adoption of only the employer identifier so far, and a compliance date still about a year away [July 2004], it will be interesting to see how the process to adopt identifiers for health plans and providers unravels. The final Employer Identifier Rule can be viewed at <http://www.cms.hhs.gov/hipaa/hipaa2/regulations/identifiers/default.asp>.

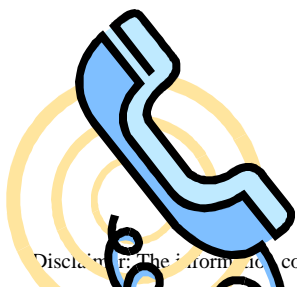
Official Contact Information

Centers for Medicare and Medicaid Services (CMS) – for Transaction and Code Set, Security, or Identifier matters

Copyright 2003 - 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.



- askhipaa@cms.hhs.gov – email address for submission of questions related to HIPAA's Administrative Simplification rules
- 1-866-282-0659 – hotline for questions related to the HIPAA Administrative Simplification regulations

Office for Civil Rights - for Privacy matters only

- OCRPrivacy@hhs.gov – email address for submission of questions related to enforcement of HIPAA's Privacy Rule
- 1-866-627-7748 – hotline for questions related to enforcement of HIPAA's Privacy Rule