

HIPAA ON THE JOB: Documenting Your Compliance with HIPAA's Privacy Rule

by Margret Amatayakul, RHIA, FHIMSS

While possibly not granting every wish on a HIM professional's privacy wish list, the final rule on privacy, issued in December 2000, comes close to addressing most of the principles we espouse. Now—perhaps—we may see more precautions, both to limit use and disclosure to healthcare purposes and to afford individuals rights to their health information.

The qualifying "perhaps" recognizes that today, more than ever before, information flows through our organizations at lightning speed. More people within an organization can easily print healthcare documents, automatically send a fax, and e-mail attachments. The risk of even well-intentioned and permitted—but not documented—disclosure is greater than ever before. And while new compliance and enforcement provisions in the final privacy rule provide the Department of Health and Human Services (HHS) broad compliance powers, the actual level of enforcement further qualifies the impact the rule may have.

Regulation vs. Legislation—What's the Difference?

Another qualification is the fact that the privacy rule is regulation, not legislation. HIPAA required the privacy issue to be handled, by default, by regulation if Congress did not pass legislation on it.

As a result, the rule only applies to information held by covered entities (a health plan, clearinghouse, or provider who transmits any health information in electronic form in connection with a transaction included in HIPAA). The final rule expands protected health information to include not only information in electronic form, but information in oral and paper form, but only when held by a covered entity. This includes providers who send paper claims to a clearinghouse or billing service that converts them to electronic form to send to a health plan. It is unknown how many providers rely solely on paper transactions and are therefore excluded from compliance.

All other organizations that have access to health information, such as employers, banks, and schools, are not covered entities. In an attempt to protect information in such organizations, the covered entity must have a business associate contract requiring the business associate to protect the health information, but putting the burden on the covered entity to see that the contract is enforced.

The final privacy rule also does not preempt more stringent state laws. Many states are passing more stringent laws to fill perceived gaps created by HIPAA. As a result, everyone will need to monitor state law, determine which is more stringent, and act accordingly.

Finally, the scope of HIPAA does not include private right of action, meaning that individuals cannot use it as a basis for a lawsuit when an egregious act occurs as a result of wrongful disclosure.

The Privacy Balancing Act

The fundamental premise upon which the privacy rule is based is that **it should be easy to use health information for healthcare purposes and very difficult to use it for any other purpose**. To carry out such a premise, HHS has had to strike a balance between individuals who want total restrictions on health information and covered entities and others who need

the information to care for patients and carry out their work.

There is also a balance between too much and too little in terms of compliance activities. A word search of the final rule and its preamble reveals that the term "reasonable" is used 256 times. "Reasonable" relates to the manner in which the rule is implemented by various sizes and types of covered entities. For example, a single practitioner is unlikely to perform sophisticated statistical calculations to de-identify information. Alternatively, a large health plan or academic medical center may be expected to apply a statistical process to ensure that information shared with employers or data for research is completely de-identified.

Perhaps the most important role an HIM professional can play with respect to HIPAA's privacy rule is that of reconciler—making sense out of the rule, interpreting it for others, and overseeing the myriad of documentation required to demonstrate compliance.

How Can I Document Compliance?

The key to compliance with the privacy rule lies in documentation. Our mantra has always been "if it's not documented, it wasn't done." To apply the rule to actual practice, it is helpful to categorize three major types of documentation that will contribute to providers' compliance. The sample checklists in this article offer guidance on what you should document to support your **compliance decisions**. (This analysis does not focus on specific requirements for health plans, nor should it be a substitute for careful reading of the rule itself.)

HIPAA does not require a specific privacy compliance plan. It does require creation of policies and procedures that are reasonably designed, taking into account size and type of activities. It also describes compliance reports that must be submitted to the secretary of HHS if compliance must be ascertained.

While such reports are not required on a routine basis, it is advisable to prepare them for internal use and in the event they are required. Documentation of all policies, procedures, communications, and actions must be retained for six years from date of creation or when last in effect, and must be kept up to date with any changes in the law. Therefore, it may be useful to develop an internal privacy compliance plan and compile a file of or index to all relevant documents, their creation and revision dates, authority for use, etc.

Although auditing is not required, it may be a good idea to periodically audit practices associated with some of this documentation to ensure compliance.

Look for more details about consent, authorization, marketing, fund raising, and notice of privacy practices in next month's "HIPAA on the Job."

A General Policy Checklist

Personnel designations (privacy officer/office responsible for receiving complaints): Job description, with authority commensurate with responsibility. It is strongly recommended that this person be knowledgeable about the content and flow of health information and able to serve in a patient advocacy role.

Minimum necessary use: Classification of persons, categorization of information, applicable conditions. This may be manifested in access control list technology for electronic information and assignment of access authorization for paper information. It is recommended that this be periodically audited.

Minimum necessary disclosures:

- Routine/recurring—Policy and procedure required; recommend periodic audits
- Other non-routine/recurring disclosures—Criteria to limit disclosure, procedure for reviewing requests

Minimum necessary requests by public officials, professional members of the work force or business associate, or researchers: Requests for information made by a covered entity when requesting information from other covered entities must be kept to the minimum necessary. It will be interesting to see how this applies to health plans when they must provide justification for disclosure of an entire medical record.

De-identification: Policy and procedure for de-identification and re-identification (code for re-identification may not be derived from information about the individual); periodic audit recommended.

Personal representative: Documentation of name and relationship recommended

Confidential communications: Policy and procedure for documentation and conditions (although provider may not require an explanation for the request). Such communications are fairly commonplace today for laboratory test reporting. It is suggested that the request for communications to be sent to an alternative location be retained as a record of compliance.

Uses and disclosures consistent with notice: Wording of notice will require attention to completeness with respect to the standard, and it should be informative without potentially inviting an avalanche of requests. It is suggested that a periodic audit be used to ensure that uses and disclosures are, indeed, consistent with the notice.

Whistleblower protections: Whistleblowers may disclose protected health information in the course of filing a complaint. Human resource policies should include provisions for such activity without retaliation.

Documents Ensuring Individuals' Rights

Documents required to comply with individuals' rights include the following:

Consent: Form should comply with the specific requirements in the rule and signed consents should be retained.

Authorization: There are specific requirements for general authorizations as well as those for specific types of disclosures.

Verification of identity and documentation of permitted disclosures where authorization is required: There should be policy and procedure for the verification process; it is suggested that documentation associated with the verification process be retained.

Use and disclosure without authorization for facility directories and involvement in care: Individuals must be informed that they will be included in facility directories, such as current census, and that a disclosure may be made to clergy or others who ask for the individual by name. Family members or others may also be provided information during the

care process. Neither of these disclosures requires authorization, but individuals must be explicitly informed and given the opportunity to object, or the provider must reasonably infer that there is no objection. While documentation is not required, if there is any doubt about the right of opportunity, it would be wise to at least document the communication. If there is a request for restriction or objection, it is recommended that this be documented. It may also be a good practice to have a standard procedure for informing individuals.

Uses and disclosures for which consent, authorization, or opportunity to agree or object is not required: Document use or disclosure for purposes of accounting for disclosure

Research where institutional review board or privacy board has approved alteration or waiver of authorization: Document alteration or waiver criteria.

Marketing and fund-raising communications without authorization: Review communications to ensure they meet requirements.

Notice of privacy practices: Notice includes specific content requirements. Document provision of notice and all revisions.

Rights to request restrictions on disclosure, access, amendment, and accounting for disclosures: Establish policy with respect to what will be accepted and what will be denied. Develop procedures and documentation processes for carrying out these requests, denials, and adjudication of denials.

Training: Retain copy of content and attendance records. Although certification of work force member attending the training and abiding by the procedures and recertification every three years are no longer required, these are solid business practices an organization may wish to consider adopting anyway.

Safeguard: The requirement to adopt administrative, technical, and physical safeguards to protect privacy essentially refers to the security proposed rule.

Complaints: Policy, procedures, and office for receipt and disposition should be established. Retain complaint and documentation of action.

Sanctions: Most providers have confidentiality agreements that indicate that breaches of confidentiality may lead to termination. It is advisable to establish more detail concerning escalation of actions and sanctions.

Documents Required to Comply with Individuals' Rights Include the following:

Consent: Form should comply with the specific requirements in the rule and signed consents should be retained.

Authorization: There are specific requirements for general authorizations as well as

those for specific types of disclosures.

- **Verification of identity and documentation of permitted disclosures where authorization is required:** There should be policy and procedure for the verification process; it is suggested that documentation associated with the verification process be retained.
- **Use and disclosure without authorization** for facility directories and involvement in care: Individuals must be informed that they will be included in facility directories, such as current census, and that a disclosure may be made to clergy or others who ask for the individual by name. Family members or others may also be provided information during the care process. Neither of these disclosures requires authorization, but individuals must be explicitly informed and given the opportunity to object, or the provider must reasonably infer that there is no objection. While documentation is not required, if there is any doubt about the right of opportunity, it would be wise to at least document the communication. If there is a request for restriction or objection, it is recommended that this be documented. It may also be a good practice to have a standard procedure for informing individuals.
- **Uses and disclosures for which consent, authorization, or opportunity to agree or object is not required:** Document use or disclosure for purposes of accounting for disclosure.
- **Research** where institutional review board or privacy board has approved alteration or waiver of authorization: Document alteration or waiver criteria.
- **Marketing and fund-raising communications** without authorization: Review communications to ensure they meet requirements.
- **Notice of privacy practices:** Notice includes specific content requirements. Document provision of notice and all revisions.
- **Rights to request restrictions** on disclosure, access, amendment, and accounting for disclosures: Establish policy with respect to what will be accepted and what will be denied. Develop procedures and documentation processes for carrying out these requests, denials, and adjudication of denials.
- **Training:** Retain copy of content and attendance records. Although certification of work force member attending the training and abiding by the procedures and recertification every three years are no longer required, these are solid business practices an organization may wish to consider adopting anyway.
- **Safeguard:** The requirement to adopt administrative, technical, and physical safeguards to protect privacy essentially refers to the security proposed rule.
- **Complaints:** Policy, procedures, and office for receipt and disposition should be established. Retain complaint and documentation of action.
- **Sanctions:** Most providers have confidentiality agreements that indicate that breaches of confidentiality may lead to termination. It is advisable to establish more detail concerning

escalation of actions and sanctions.

Documentation to Protect Contractual Obligations

Documentation required to protect contractual obligations is the third category that a provider should ensure exists. These include:

- ❑ **Business associate contract:** Contract must establish permitted and required uses and disclosures and safeguard information. Providers will have many associates, from contract transcription services that clearly have access to protected health information, to information systems vendors who may have dial-in access for troubleshooting and providing updates. A data flow diagram may help identify all direct business associates. Although separate contracts are not required for downstream recipients of protected health information, identifying these can help ensure that the associates' agents are addressed in the contracts.
- ❑ **Healthcare component of hybrid entity:** Document relationship and responsibilities of covered entity. Ensure that plan agreement is updated to incorporate new restrictions on disclosure, including use of summary information.
- ❑ **Affiliated covered entities:** Many providers have business ventures. If these are other providers (such as a retail pharmacy or home health agency), document designation of affiliation and responsibilities with respect to joint notices and other documents.
- ❑ **Multiple covered functions:** Many providers also operate health plans. Document relationships and responsibilities.
- ❑ **Mitigation of harmful effect of a use or disclosure:** Establish a tracking mechanism and procedure for action.

Margret Amatayakul is the founder and president of MargretA Consulting, LLC, an independent consulting firm based in Schaumburg, IL. She can be reached at margretcpr@aol.com.

Copyright © 2001 American Health Information Management Association. All rights reserved. All contents, including images and graphics, on this Web site are copyrighted by AHIMA unless otherwise noted. You must obtain permission to reproduce online any information, graphics, or images from this site. You do not need to obtain permission to cite, reference, or briefly quote this material as long as proper citation of the source of the information is made. The above text was originally published in the Journal of AHIMA. Please contact Publications at publications@ahima.org to obtain permission. Please include the author, title, and Journal issue of the article you wish to reprint in your request.

