Reinhart

HIPAA Privacy Rule

On December 28, 2000, the Department of HHS published the Final Rule establishing Standards for Privacy of Individually Identifiable Health Information. This Rule will require organization-wide changes in how patient information is handled; it sets forth extensive and complex limitations on the use of individually identifiable information and applies to virtually all health care providers, health plans (including self-funded employers) and clearinghouses. This Rule is part of HIPAA's Administrative Simplification provisions and most providers, health plans, clearinghouses and their business associates will be subject to its sweeping requirements. This may seem like the distant future, but given the complexity and comprehensiveness of the regulations, the time to start is now. While there is some discussion regarding what effect the new administration will have on the implementation of these requirements and the effective date, it is virtually certain that hospices, along with all other health care providers, will be required to institute major changes in how individually identifiable patient information is gathered and transmitted.* The following is a summary of key issues:

The Privacy Rule Covers All Records. The Final Rule defines Protected Health Information to be individually identifiable health information transmitted or maintained electronically or transmitted or maintained in any other form or medium. This means that all records containing individually identifiable health information maintained by a covered entity are covered by the regulation. In order for the records of an entity to be subject to this rule, the entity must be a "covered entity" as defined in the regulation. Covered entities include health plans and clearinghouses, as well as health care providers who transmit any health information in electronic form

Consent Required for Treatment, Payment or Health Care Operations. The Final Rule requires consent prior to releasing protected health information for treatment, payment or health care operations. The Rule contains requirements for the form and content of a consent. For example, if a consent is combined with other forms of legal permission, it must be visually and organizationally separate from the legal permission and it must be separately signed and dated. A consent that does not meet the content requirements of the Final Rule is not a valid consent. Notably, a health care provider may condition treatment on the provision by an individual of consent to release protected health information for treatment, payment or health care operations.

POSTED:

Mar 4, 2001

RELATED PRACTICES:

Health Care
https://www.reinhartlaw.com/practices/health-care

RELATED SERVICES:

Hospice and Palliative Care
https://www.reinhartlaw.com/services/hospice-and-palliative-care

It is important to note that consent to release for treatment, payment or health care operations is not the same as authorization to release protected health information. "Authorization" is a much more detailed and involved process.

Marketing and Fundraising. The Rule contains a general prohibition against the use of protected health information for marketing or fund raising without authorization, and defines conditions which, if met, allow a covered entity to use protected health information without first obtaining an authorization. This will be important for health care providers who use patient lists in their fundraising and marketing efforts.

Employment Related Actions. The Rule clarifies that employers who sponsor health plans, including self-insurers, cannot access health information for employment related actions or in connection with other benefit plans without obtaining specific consents.

Enforcement. The DHHS Department for Civil Rights will implement and enforce the rules in coordination with the Department of Justice in the event of criminal violations. It is important to note that there are significant civil as well as criminal penalties for violation of the privacy regulations.

Preemption of State Law. The Rule provides that the Federal law concerning privacy and confidentiality of protected health information takes precedence over state law except in numerous circumstances set forth below:

- State law is more stringent;
- The Secretary of DHHS determines that the State law is necessary to prevent fraud and abuse, to regulate insurance and health plans, for State reporting on health care delivery or costs, for purposes of serving a compelling need related to public health, safety or welfare, or has as its principal purpose the regulation of the manufacture, distribution, registration, dispensing or control of any controlled substances;
- State law provides for reporting of disease or injury, child abuse, birth, or death, or for the conduct of public health surveillance, investigation or intervention;
- State law requires a health plan to report, or provide access to, information for purposes of management audits, program monitoring and evaluation, or the licensure or certification of facilities or individuals.

This provision means that implementation of the Federal Rule will require careful comparison to state law. In some circumstances,state law will control and in other circumstances the Federal law will control.

Business Associates. Under the Rule, a Business Associate is either:

- An entity that performs a function or activity on behalf of a covered entity involving use or disclosure of individually identifiable health information and includes claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or
- An entity that provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation or financial services to or for a covered entity where provision of the service involves disclosure of individually identifiable health information.

A covered entity may disclose protected health information to a Business Associate if the covered entity has a written agreement with the Business Associate containing assurances that the Business Associate will appropriately safeguard the information. The Final Rule sets forth the terms and conditions that must be contained in a Business Associate contract.

Where to Begin **

Complying with the HIPAA Administrative Simplification requirements will be a long and often complex process, although advocates insist that, eventually, it will simplify your claims administration and make your office more efficient. Complying will require you to work with experts such as technical people versed in the subjects of security and, potentially, consultants or attorneys. Here are some things you can start doing right now.

Educate Your Board and Upper Management. The Board of Directors and key staff face considerable personal liability if your organization is not compliant with HIPAA. Now is the time to create "ownership" in your compliance program at the highest levels of the organization.

Assign Someone to Act as Your Privacy Officer. This is required by the regulations and there is no reason to hesitate in appointing this person now to oversee compliance. Your privacy officer can begin the process of becoming well versed in the law and how to comply and, at your discretion, also can act as the interface with outside consultants. In addition, when he or she is up to speed, this person can start increasing awareness of everybody in the organization with written material and educational programs.

Conduct a "Gap Analysis". This is, perhaps, the most critical thing you can do

now to start on the road toward HIPAA compliance. A gap analysis refers to reviewing how your hospice currently manages protected health information compared to how you must handle that information to comply with the new regulations. That, in turn, will help you focus your efforts. Some providers hire consultants to assist with this process, either on-site or as a desk audit. This preliminary review, covering the "gaps" between current practice and what HIPAA will require, should cover:

- Patient information. Who has access to claims data and charts? Where is the fax machine and who has access to it? You will violate HIPAA if a record left in a fax machine is read by somebody who should not have access to it. Do you have patient names in open areas in the office? A walkthrough of your hospice office can pinpoint HIPAA risk areas.
- Policies and procedures. Do you have policies governing confidentiality of patient information? Is there a formal training program? Are there sanctions for failure to follow the policies? In consultation with human resources personnel, gather all relevant policies and procedures, including your employee handbook, for review and updating.
- Contracts. It is critical to make sure your "business associates," comply with HIPAA. First, identify those parties with whom you share patient records. Then, you must review not just how records flow from your office to your business associates and what they do with them, but also all contracts you have with them. The regulations require you to have written contracts that must include specific language assuring HIPAA compliance. Have your attorney draft necessary amendments to your existing contracts.
- Consents and authorizations. Have your attorney review and revise your current consent forms and authorization forms and your current procedures to conform with HIPAA. The rule is very specific regarding the language and use of these forms.
- Communicate with your vendors to make sure they have plans to comply with security requirements and standards for electronic transmission of patient information.

Conclusion

This article touches on only a few provisions of the HIPAA privacy and confidentiality regulation. Implementation will require legal understanding of the rule and it will require careful thought about how the regulation actually applies. Becoming compliant with HIPAA "Administrative Simplification" will be anything

but simple, requiring you to extensively rework virtually every aspect of how you handle patient information.

The federal government insists that HIPAA will simplify your record keeping and, maybe in the long run, it will. At the very least, it will bring about a more systematic approach to handling and using health care data. It also will increase the confidence of your patients that they and their private information are being protected.

The good news is that you have enough time to make sure your hospice complies with HIPAA. The bad news is that complying will be time-consuming, complex and costly. And the ugly news is that failure to comply could result in stringent civil and criminal penalties. Because of those reasons, and because there are no one-size-fits-all solutions for becoming HIPAA compliant, the time to start complying is now.

---

* The current effective date of the Rule is April 14, 2001, with implementation for most covered entities set for April 14,
2003. The new administration may make certain changes to the Rule. The Rule for Electronic Transmission Standards will
not change and compliance is required by October of 2002.
** The following is excerpted in part from an article I co-authored for EyeNet, a publication of the American Academy of
Ophthalmologists.