



Insurance Solutions For Healthcare Providers

Vol. 21 No. 3

Third Quarter 2009



Inside This Issue:

▶ What Physicians Need to Know About the “Red Flags” Rule

Information in this newsletter does not establish a standard of care, nor is it a substitute for legal advice. The information and suggestions contained here are generalized and may not apply to all practice situations. First Professionals recommends you obtain legal advice from a qualified attorney for a more specific application to your practice. This information should be used as a reference guide only.

First Professionals Insurance Company is Florida's Physicians Insurance CompanySM and the endorsed carrier for professional liability insurance by 23 county medical societies, 15 specialty societies, and two statewide associations in Florida.

NEWS & VIEWS

The Impact of the Federal Stimulus Package on Healthcare Delivery



By Cliff Rapp
Vice President
Risk Management

Identity theft is a spiraling international problem. While it is often difficult to detect when the identity of a patient is stolen, measures to protect the identity and privacy of all

patients continue to evolve globally. One example is the Federal Stimulus Package, which sets forth substantial changes to requirements for the protection of health information privacy and security under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Virtually every medical practice is affected by these latest revisions. Notification requirements of a privacy breach and restriction and accounting of disclosures in the face of increased enforcement measures require that physicians become acquainted with the new regulations and the necessary compliance measures.

Passage of the American Recovery and Reinvestment Act of 2009 (ARRA), often referred to as the “Federal Stimulus Bill”, resulted in myriad HIPAA revisions. These revisions were enacted in response to a number of factors; the evolution of new entities holding personal health information, an absence of privacy breach notification requirements, and a lack of control over business associates – including inadequate enforcement. While the revisions primarily pertain to privacy measures of electronic health records, the existing preemption principles of HIPAA still apply. The Secretary of the

Department of Health and Human Services (DHHS) is responsible for enacting HIPAA rules to conform to ARRA provisions. Consequently, additional HIPAA revisions should be anticipated.

The majority of HIPAA revisions apply to “covered entities” (defined as a health plan or payor, a healthcare clearing house, billing service, or any healthcare provider that transmits any healthcare information in electronic form) and their “business associates” (essentially anyone who uses or discloses a patient’s personal health information in order to perform a function necessary to help carry out a healthcare function) and serves to modify HIPAA privacy and security rules applicable to electronic health records. These revisions may be summarized as follows:

Compliance

Covered entities must initiate a written, breach notification policy and procedures plan in addition to the HIPAA compliance plan. The new

“ ..increased enforcement measures require that physicians become acquainted with the new regulations and the necessary compliance measures.”

Continued on next page

Continued from front

provisions require that specific procedures entailing breach notification include documentation of staff training, provide an accounting of disclosures and contain a corrective plan in the event of a privacy breach.

Business Associates

Business Associates (BAs) must fully comply with HIPAA Security and Privacy rules. Penalties for noncompliance apply to BAs who must secure their own business associate agreements. Health information exchanges, such as regional health information exchanges are considered BAs.

Breach Notification

Breach of personal health information (PHI) privacy or security is the responsibility of the covered entity. An individual must be notified if the breach is of unsecured PHI, such as unencrypted electronic records. Each individual affected by the breach must be notified in writing, within 60 days of discovery. An annual log must be maintained, and reported to DHHS. Covered entities are required to adhere to the written notification procedures contained in their HIPAA compliance plan.

Disclosures Accounting

An accounting of all PHI disclosures, including those disclosures made for payment, treatment and operations must be maintained. Furthermore, all disclosures must be limited to the minimum necessary – as defined by DHHS.

Disclosure Restrictions

Patients may restrict disclosure of PHI to their health plan, insurer or managed care organization if the PHI pertains to health information that was fully paid for by the patient.

Individual Rights

Patients have the right to obtain their electronic medical records electronically and may not be charged for more than the labor costs incurred. Patients may also take civil action against a BA, in addition to a covered entity, for security and privacy breach occurrences.

Enforcement, Penalties, and Audits

Government enforcement capabilities of HIPAA security and privacy violations have been significantly

enhanced in tandem with increased governmental monetary fines and penalties. Patients may also initiate civil actions seeking monetary damages in addition to governmental penalties. State Attorneys General can sue in federal district court for such civil damages and are free to award court costs and attorney fees in addition to monetary damages. Consequently, broadened financial incentives and increased legal action may result. Criminal penalties for wrongful disclosure of PHI apply to individuals whether employees or not of a covered entity. The DHHS is required to perform periodic audits of both covered entities and their business associates. Many of the HIPAA revisions implemented as a result of the ARRA remain under governmental rulemaking review with varying phase-in dates and compliance deadlines. For these reasons, contemporaneous legal or risk management guidance should be sought.

Risk Management Guidelines

- Prospectively seek legal or risk management guidance
- Become fluent in HIPAA terminology
- Educate and train all levels of staff
- Review and revise outdated HIPAA compliance measures
- Revise patient information forms, consents and authorizations
- Ensure BA agreements are compliant
- Remain current – access professional, governmental, and legal informational websites
- Diary applicable ARRA effective dates
- Anticipate continued revisions and timeframes

References

- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- American Recovery and Reinvestment Act of 2009 (ARRA)
- 45 C.F.R. § 164.308 – Regarding administrative safeguards to protect ePHI;
- 45 C.F.R. § 164.310 – Regarding physical safeguards to limit physical access to ePHI;
- 45 C.F.R. § 164.312 – Regarding technical safeguards for electronic information systems that control access to ePHI;
- 45 C.F.R. § 164.316 – Regarding reasonable and appropriate policies, procedures and documentation requirements of the HIPAA Security Rule as it relates to ePHI.
- American Recovery and Reinvestment Act of 2009, H.R. 1, 111th Cong. § 13400(1) (2009) ■

What Physicians Need to Know About the “Red Flags” Rule

By: Cliff Rapp, LHRM, Vice President, Risk Management



Most physicians are aware of the Federal Trade Commission “Red Flags” Rule pertaining to patient identity theft protection standards. Due to the relative depth of the Rule, it is recommended that a reference manual be established and understood by all affected medical practices, ideally as an addendum to current HIPAA reference material. Failing to comply with the Rule could prove costly.

The Federal Trade Commission (FTC) issued rules that require “financial institutions” and “creditors” holding consumer or other “covered” accounts to develop and implement an identity theft prevention program.

Enforcement of these rules, referred to as the “Red Flags” Rule (Rule), is effective November 1, 2009. The Rule affects individual physicians, physician groups, hospitals and other healthcare organizations that qualify as a “creditor”, which is defined as “any person who regularly extends, renews, or continues credit” or “defers payment of a debt.” Healthcare practitioners routinely extend “credit” by performing services and “billing” the patient at a later date either through sending a claim to the insurance company and/or accepting partial payment or co-pays and thus have been interpreted to be a “creditor” by the FTC under the Rule.

The Rule requires implementation of a written Identity Theft Prevention Program (Program). The Program must be appropriate to the size and complexity of the practice and designed to detect, prevent, and mitigate identity theft in connection with the opening of a “covered account” or any existing covered account. A covered account is defined to include an account “... designed to permit multiple payments or transactions...”.

Most physicians and group practices fall under the FTC’s definition of a creditor because they generally do not collect payment at the time a service is rendered and often hold off billing patients in full.

The Program must include reasonable policies and procedures to identify and incorporate red flags, detect red flags, respond appropriately to any red flags that are detected, and periodically update the Program. Office managers and administrators should assiduously enforce compliance measures established by the practice.

The initial written Program must be approved by a board of directors, appropriate committee of the board, or a designated employee at the level of senior management in the oversight, development, implementation, and administration of the Program. Training of staff must be included in order to effectively implement the Program and provide oversight.

Failure to comply with the new Rule subjects a physician’s practice to monetary penalties and civil litigation, including:

- Federal Enforcement – up to \$2,500 per violation;
- State Enforcement – up to \$1,000 per violation, in addition to recovery of attorney’s fees; and
- Civil Liability – Each patient may be entitled to recover actual damages sustained from a violation.

Continued on next page

Continued from previous page

Establishing a reference manual and initiating staff training are fundamental risk management measures. In light of the potential for civil monetary penalties and fines, failing to comply with the requirements of the Rule could prove to be a costly mistake.

First Professionals Insurance Company (First Professionals) has developed material to help clarify the Rule pertaining to patient identity theft protection standards. The packet contains an overview of the new Rule, risk management guidelines, and website references. It also contains several forms and templates to assist with compliance measures.

Due to the relative depth of the Rule, First Professionals suggests that you establish a reference manual for your office, ideally as an addendum to your current HIPAA reference material. This latest material, along with any other additional information you obtain, can be a vital resource in implementing protection against patient identity theft and compliance with the Rule.

Please note that the complete Rule package, including compliance measures, is available within the risk management link on our website, www.firstprofessionals.com. If you have any questions about this material or require additional copies, contact a First Professionals risk management consultant at (800) 741-3742, ext. 3016 or send an e-mail to rm@fpic.com.

Additional Information

- To file a complaint visit www.ftc.gov or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261
- Federal Trade Commission, Red Flags Rule. Title 16 CFR §681.1 and §681.2
- RedFlags@ftc.gov.
- www.ama-assn.org/go/pmc ■

PRESRT STD
U.S. POSTAGE
PAID
Permit No. 1729
Jacksonville, FL

P.O. Box 44033 Jacksonville, FL 32231-4033
800-741-3742 • www.firstprofessionals.com

