

# Preventive Action

Quarterly Risk Management Newsletter for Policyholders of FPIIC

Fourth Quarter 2009

Vol. 22, No. 4

## The Impact of the Federal Stimulus Package on Healthcare Delivery

By Cliff Rapp, LHRM, Vice President, Risk Management  
First Professionals Insurance Company



*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 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.

“ While the revisions primarily pertain to privacy measures of electronic health records, the existing preemption principles of HIPAA still apply. ”

### 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

*continued on next page*

### TABLE OF CONTENTS

Page 3	Mandatory Reporting – Medicare Secondary Payer Act
Page 4	New HIPAA Security Electronic Security Tool
Page 5	Case Study: Inadequate Communication Leads to Stroke
Page 6	Legal FAQs



First Professionals Insurance Company



First Professionals Insurance Company publishes Preventive Action on a quarterly basis as a service to policyholders. Information in this publication does not establish a standard of care, nor is it a substitute for legal advice. The information and suggestions contained in this newsletter are generalized and may not apply to all practice situations. First Professionals Insurance Company recommends you obtain legal advice from a qualified attorney for a specific application to your practice. The information should be used as a reference guide only.

For comments, questions or to obtain additional copies contact the First Professionals Insurance Company Risk Management department at 800-741-3742, ext. 3016.

Cliff Rapp  
Vice President of Risk Management  
Editor-in-Chief

Linda Blythe  
Risk Management Consultant

Ruth Lopes  
Risk Management Consultant

Joseph Putz  
Risk Management Consultant

Sandra C. Strickland  
Risk Management Consultant

First Professionals Insurance Company  
1000 Riverside Avenue, Suite 800  
Jacksonville, FL 32204

800-741-3742  
Local 904-354-5910  
Fax 904-354-6132

[www.firstprofessionals.com](http://www.firstprofessionals.com)

Copyright 2009 by First Professionals Insurance Company Inc. All rights reserved. No part of this publication may be reproduced or transmitted in any form.

First Professionals Insurance Company is Florida's Physicians Insurance Company and the endorsed carrier for professional liability insurance by 22 county medical societies, 15 specialty societies and two statewide associations in Florida, including the FMA and FDA. Premium discounts may be available to members in good standing.

continued from page 1

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 business associate, 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, authorizations
- Ensure BA agreement is compliant
- Remain current – professional, governmental, and legal informational websites
- Diary applicable ARRA effective dates
- Anticipate more 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)* –

# Mandatory Reporting Medicare Secondary Payer Act

By Cliff Rapp, LHRM, Vice President, Risk Management  
First Professionals Insurance Company  
Anesthesiologists Professional Assurance Company



**Effective January 1, 2010**, the Medicare Secondary Payer Act [42 U.S.C. 1395y(b)(7) & (8)] requires that all liability carriers report payments made to any Medicare plaintiff/claimant to the Center for Medicare and

Medicaid Services (“CMS”). This reporting requirement may also apply to payments made directly by a physician and by “self-insured” physicians.

**First Professionals Insurance Company will report payments made on behalf of its policyholders to CMS. For payments made by a physician directly to a claimant, the physician may be responsible for reporting to CMS. See reporting information below.**

Reports must be submitted to CMS in *electronic* format only, on the CMS website [www.cms.hhs.gov/MandatoryInsRep](http://www.cms.hhs.gov/MandatoryInsRep). However, the electronic reporting may be waived when there is no method available for the submission of claims (a) in an electronic format; (b) for a provider of services with fewer than 25 full-time equivalent employees; or (c) for a physician, practitioner, facility, or supplier (other than provider of services) with fewer than 10 full-time equivalent employees.

**Reporting thresholds** by payment year and amount are:

2010 - over \$5000.00  
2011 - over \$2000.00

CMS will assign each registered liability carrier a specific date for reporting every quarter. If a physician makes a payment directly to a plaintiff/claimant which meets the reportable threshold, CMS should be contacted as soon as possible regarding how and what to report. Generally, the report date is determined by the date of settlement, date of verdict, or date of appeal result, not the date that payment is made.

**Factors to consider in determining whether you must report a payment:**

1. Is the plaintiff/claimant a Medicare recipient?

Look at the entitlement at the “time of incident”:

- Persons who have reached age 65 and are entitled to receive either Social Security, widows or Railroad Retirement Benefits;

- Disabled persons (totally disabled) receiving SSDI;
- Persons of any age who have received Social Security, widows or Railroad Disability Benefits for 25 months (this may apply to disabled minors/adults);
- Persons with end-stage renal disease who require dialysis treatment or kidney transplant; and
- Working persons over age 65 that are not eligible for either Social Security or Railroad Retirement Benefits who purchase Medicare coverage by monthly payment or as active employees for an employer of 20 or more employees.

2. Is the payment over the dollar threshold for the year it was made?

**If you must report, how and what do you report?**

Generally, unless a waiver is received for *electronic* reporting, every report must contain the following information for each claimant:

- Name of claimant (with middle initial);
- Social Security number (HICN when available);
- Complete address;
- Telephone number;
- Gender;
- Date of birth;
- Date of death, if applicable;
- Full contact information on any estates, siblings or other representative claimants, if applicable;
- Full contact information for claimant’s attorney including tax ID numbers, if applicable;
- Dates and the nature of any injuries, including whether the injury involved an allegedly defective product, if applicable;
- Information detailing any resolution or settlement of a claim, with a focus on explaining whether the claim was contested or not, and whether the primary payer has assumed ongoing responsibility for medical costs associated with the claim.

There are very steep **fin**es (\$1000 per day, per claimant) for failure to report pursuant to these requirements.

The reporting requirement does **not apply to Medicaid** recipients.

Contact CMS at [www.cms.hhs.gov/MandatoryInsRep](http://www.cms.hhs.gov/MandatoryInsRep) or by phone at 800-999-1118. Additional information may also be obtained by contacting the First Professionals Risk Management Department at 800-741-3742 ext. 3016 or via e-mail to [rm@fpic.com](mailto:rm@fpic.com). •

# Risk Management Products & Services

Available at no charge to policyholders

## New HIPAA Electronic Security Tool

Protecting a patient's Electronic Personal Health Information (EPHI) is both a HIPAA requirement and important fiduciary duty. Measures to prevent the risk of inadvertent disclosure of EPHI need not be complicated or costly. To assist with such risk management efforts, First Professionals has developed a HIPAA security tool available at no cost to our policyholders.

Utilizing the HIPAA Security Audit Tool Sticker to complement an assessment of electronic security compliance is a fundamental, yet effective risk management measure. The sticker should be placed on an employee's computer when found logged-on and unattended, but accessible to others – a clear HIPAA security violation. Ideally, the employee's computer access should then be locked. The employee should be required to sign the warning violation sticker in order to regain access to their computer.

Use of the HIPAA Security Audit Tool Sticker is designed to raise employee awareness of electronic security and avoidable HIPAA violations. Assessments should be randomly performed to ascertain that all levels of staff are adhering to mandatory HIPAA privacy and security measures. Violations of the new electronic security regulations are subject to costly civil and monetary penalties that are not covered by most insurance policies.



**WARNING  
HIPAA VIOLATION**

Dear \_\_\_\_\_,

Your computer was left unlocked while you were away from the desk. Please sign this form and bring it to \_\_\_\_\_ to have your computer unlocked.

I acknowledge that securing this computer is my responsibility and I have violated security policies. I agree to adhere to all computer security measures.

\_\_\_\_\_  
Name

\_\_\_\_\_  
Date

To obtain a free set of the HIPAA Security Audit Tool Stickers, policyholders of First Professionals Insurance Company should contact the Risk Management Department at (800) 741-3742, ext. 3016 or [rm@fpic.com](mailto:rm@fpic.com). •

# Case Study: Inadequate Communication Leads to Stroke

*Editor's Note: This case analysis reflects an actual First Professionals' case.*

## Case Analysis

The patient, a 65-year-old male, underwent prosthetic cardiac valve placement and was placed on an anticoagulation medication under management by his internist. The patient returned monthly to the internist's office and/or clinic lab for coagulation panels and dose regulation. The patient subsequently missed several lab visits, which went unnoticed by the internist until six months later when the patient was treated for a urinary tract infection and his chart was reviewed. A coagulation panel was then done and a dosage adjustment was necessary. The internist instructed the nurse to reduce Coumadin by one milligram daily and call the patient with the new regimen. The RN phoned the patient's home and relayed instructions to the patient's wife. Two weeks later the patient was admitted via the ER with a diagnosis of ischemic stroke, sustaining significant neurological and cognitive deficits. It was determined that the patient's wife had written "reduce Coumadin to one milligram daily." Unfortunately, the RN did not document her telephone call with the instruction to reduce the dose by one milligram daily, resulting in a question of fact.

## Risk Management Discussion

*Stroke remains a leading cause of death and malpractice claims against physicians. Few medical specialties are immune. Often, these malpractice claims have little to do with the competency of the physician but rather faulty monitoring and system failures. Frequently, the physician's indefensibility is attributed directly to inadequate management of anticoagulation therapy. Loss prevention measures shown to reduce errors, deter lawsuits and preserve defenses necessary to defeat unavoidable claims include:*

- Identify patients at risk for stroke according to established clinical standards.
- Identify all patients for whom an anticoagulation medication is indicated.
- Document a specific reason or contraindication whenever a high-risk patient is not on an anticoagulation medication.
- Educate patients about the implications of anticoagulation therapy. Document these efforts.
- Create written policies and guidelines pertaining to patient identification and documentation.
- Establish written procedures for monitoring patients on anticoagulation therapy and follow them.
- Discuss potential risks and benefits of therapy with the patient and/or caregiver.
- Obtain informed consent.
- Document patient refusal or noncompliance.
- Keep AF patients consistently in INR 2.0 – 3.0 range.
- Commit to appropriate monitoring system.
- Utilize an anticoagulation medication monitoring regimen system.
- Seek legal or risk management advice when uncertainty arises. —

*This information 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 Company and the endorsed carrier for professional liability insurance.*

## Legal FAQs For information specific to your state of practice, contact First Professionals' Risk Management department



### **What action should be taken when a medical error is suspected or occurs?**

Contact FPIC's Risk Management Department for guidance as soon as possible. Make no admissions of liability. Federal and/or state reporting requirements under strict time constraints may apply. Always attempt to discuss the situation with personal counsel or FPIC before meeting with hospital risk management.

### **What action should be taken when a patient is noncompliant or refuses to undergo diagnostic studies, care, or treatment?**

Document your recommendations and the patient's noncompliance. Advise the patient of the potential consequences of their noncompliance or refusal and

document your discussion. Confirm the patient's noncompliance, your subsequent discussion and the potential consequences in a letter to the patient sent certified mail, return receipt requested and send a copy of the letter by regular mail as well. Consider withdrawing from the patient's care, but first review the language of any managed care contracts that may apply to the situation and seek guidance from FPIC's Risk Management Department or personal counsel. If you practice in a group setting, it may be necessary to withdraw on behalf of others in the group and the practice itself.

### **When a patient leaves the hospital AMA (against medical advice) is the physician-patient relationship automatically severed?**

No. The patient can assert that the AMA was purely for some aspect of treatment, such as surgery or physical therapy, but not all care and treatment. Always document the record in the case of an AMA and send a letter to the patient confirming their forfeiture of care and the potential consequences of their actions. Ask the patient to reconsider, but do not deny the patient access to ongoing care. Consider terminating the physician-patient relationship. Depending on the circumstances, seek legal guidance before taking such action.

### **What is arbitration and what benefit does it provide?**

Arbitration is the submission of a dispute to one or more impartial persons for a final and binding decision. Through arbitration, patients and physicians both benefit because they are able to more promptly resolve malpractice claims and for less cost to each party. It is also believed that arbitration panels will help to avoid unreasonable jury awards, thereby further lowering costs. These cost savings would positively impact professional liability rates and the cost and availability of healthcare services.

### **What are the legal differences between a nurse practitioner and a physician assistant?**

Generally, a nurse practitioner's scope of practice varies from state to state. In many states, they are allowed to practice independently. However, NPs often practice under the guidance of a licensed physician. A physician assistant is required to practice medicine under a physician's supervision and can practice only under a physician's license. A PA can conduct physical exams, diagnose and treat illnesses, order and interpret tests and in many states, write prescriptions. •