



Bentley  
Insurance  
Group

THE *Best* COVERAGE  
FOR THE *Best* DOCTORS.

# Preventive *Action*

Quarterly Newsletter for Policyholders  
**November 2009**

## Bentley Insurance Group Offers the Best Insurance for the Best Physicians



defense costs that are included as part of coverage, including defense for allegations of misconduct brought by regulatory agencies. Free tail coverage is available for physicians who retire (with no age restriction) after five years of continuous coverage. Unlike some of our competitors, we also allow policyholders the option to consent to settle - you decide to defend or settle.

When you become insured with First Professionals Insurance Company (First Professionals), you become a member of Bentley, formed for the specific purpose of providing affordable, quality medical malpractice insurance to preferred physicians and surgeons practicing in Illinois.

In addition to the products and services offered by First Professionals, Bentley has established a new partnership with ELM Exchange, Inc. (ELM). This risk management program not only helps physicians improve their practice, it offers CME credits and discounts on their insurance premium.

The ELM program allows policyholders of First Professionals to complete three courses per year, totaling 5.25 CME credit hours at NO COST and receive a 5% discount on their premium. Each year at least three courses will be available to you online through the program.

With over 30 years of experience, First Professionals has the expertise to provide the best protection for doctors. In addition to affordable premiums, the company offers benefits for its policyholders, including the ELM program, that are unmatched in the industry. Policyholders can also depend on the financial strength of First Professionals which is validated by an A.M. Best rating of A- (Excellent) and Fitch rating of A- (Strong).

For more information about the products and services offered by Bentley, please visit [www.bentleyinsurancegroup.com](http://www.bentleyinsurancegroup.com) or contact your agent. ▶

Now entering its third year of offering coverage for doctors, Jack Ahern, president of Bentley says, "We couldn't be happier with the positive reception from the brokerage and medical community here in Illinois. Our claims-made program has been a trendsetter in this market by offering exceptional coverage for Illinois physicians."

Coverage benefits include competitive premiums with flexible payment plans,

### TABLE OF CONTENTS

Page 2 The Impact of the Federal Package on Healthcare Delivery

Page 4 New HIPAA Electronic Security Tool

“With over 30 years of experience, First Professionals has the expertise to provide the best protection for doctors.”



First Professionals Insurance Company



**Bentley  
Insurance  
Group**

## The Impact of the Federal Package on Healthcare Delivery

*The information below 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.*

*By Cliff Rapp, LHRM, Vice President Risk Management, FPIC*

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 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.

### **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

**Continued on next page**

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 HHS.

### 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 or not they are employed by 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)

*Cliff Rapp is a licensed healthcare risk manager and Vice President for Risk Management of First Professionals Insurance Company, a leading professional liability insurer. Mr. Rapp is widely published and a national speaker on loss prevention and risk management. ▶*



## 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.

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

**WARNING  
HIPAA VIOLATION**

Dear \_\_\_\_\_

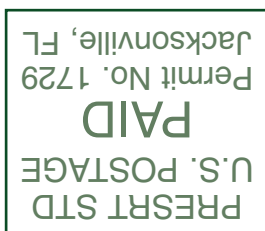
Your computer was left unlocked while you were away from the desk. Please sign this form and bring it to \_\_\_\_\_ to have your computer unlocked.

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

**THE *Best* COVERAGE FOR THE *Best* DOCTORS.**



550 W. Van Buren, Suite 1200 • Chicago, IL 60607  
 (800) 984-7570 • [www.bentleyinsurancegroup.com](http://www.bentleyinsurancegroup.com)

