ANESTHESIA & the LAW
A Risk Management Newsletter
DECEMBER 2014 – ISSUE 40
PPM

Emerging Trends in Anesthesia: Cyber Liability

Recent national media attention has highlighted potential liability arising from the unauthorized disclosure of personal health information (PHI). Following one of the largest cyber attacks on a major health system's computer network involving PHI of 4.5 million patients, the Federal Bureau of Investigation (FBI) recently warned the health care industry is a likely target for increased cyber attacks. The FBI also warned that health care providers' computer security systems were more vulnerable to hacking than other private industry sectors such as retailers and financial institutions.

In the last year, national media stories reported significant health care related breaches prompting notification to approximately 840,000 Blue Cross Blue Shield members when two laptops containing PHI were stolen from its New Jersey headquarters. Media coverage also included the theft of two laptops from a California hospital system that compromised the PHI of 729,000 patients, including social security numbers. According to a 2014 study on patient privacy and data security, lost or stolen computing devices cause 49% of cyber breaches.*

Experts in cyber liability indicate cyber criminals frequently use stolen medical and personal information to impersonate patients either to obtain prescriptions for controlled substances or to commit financial fraud. Cyber criminals are able to sell stolen patient information and are typically paid a premium of approximately $20 for health insurance information compared to $1 or $2 for U.S. credit card numbers.

Cyber Liability for Anesthesiologists Expanded

Traditionally, anesthesiologists and their practices do not appear to have been the focus of cyber attacks or the unauthorized disclosure of PHI. According to Wade Willard, PPM's Vice-President for Claims, this may be largely due to the nature of anesthesia practice. According to Willard, "the majority of our insured anesthesiologists continue to work in a hospital or surgery center setting where the facility is primarily responsible for gathering, storing and securing patients' PHI."

More recently, as anesthesia practices have expanded to serve multiple facility locations and reliance on electronic medical records and systems has increased, anesthesiologists may need to re-evaluate the adequacy of their efforts to secure PHI. Expansions to the scope of practice including the proposed American Society of Anesthesiologists (ASA) Perioperative Surgical Home practice model may also alter level of PHI anesthesiologists control or are required to access and protect in their systems.

Cyber liability risks for anesthesiologists may also increase due to regulatory incentives to promote the adoption of electronic health record (EHR) systems, technological enhancements, including the movement from client/server systems to internet server platforms, and anesthesiologists' escalating dependence on mobile technology solutions such as laptops, smartphones, tablets and other personal electronic devices used to support their anesthesia practice.

Other Potential Breaches

In addition to high tech data breaches, health care organizations also remain susceptible to breaches related to the loss of paper records. Preferred Physicians Medical (PPM) has noted several reported incidents of medical records being disposed of in non-secure trash receptacles or public recycling containers, as well as security breaches related to lapses during storage, shredding or transmitting records by mail.

Other electronic and privacy exposures include, but are not limited to, health care providers who do not encrypt sensitive data, increased use of electronic databases to store vast amounts of sensitive information, outsourcing information technology, and rogue employees who steal data.

Increased Federal and State Regulatory Scrutiny

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule protects all *"individually identifiable health information"* held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule defines this information as "protected health information (PHI)." HIPAA governs how health care organizations can use, collect and disclose private information. HIPAA also requires health care providers to implement "appropriate" administrative, technical and physical safeguards to protect private information. Additionally, HIPAA requires covered entities to implement employee training on how to properly safeguard private information.

* "2014 Cost of Data Breach Study." *Ponemon Institute*, May 2014. *http://www-935.ibm.com/services/us/en/it-services/security-services/cost-of-data-breach/*

Under the Health Information Technology for Economic and Clinical Health, enacted as part of the American Recovery and Reinvestment Act of 2009, (HITECH Act), the U.S. Department of Health and Human Services developed breach notification requirements that all covered entities and business associates must follow in the event of a breach of unsecured PHI, including electronic PHI or ePHI. The HITECH breach notification rules, as amended by the HIPAA Omnibus Rule published in January 2013, define a breach as the acquisition, access, use or disclosure of PHI in an impermissible manner that compromises the security or privacy of PHI.

Additionally, forty-seven states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring private or government entities to notify individuals of security breaches of information involving personally identifiable information.

Security breach laws typically include provisions regarding who must comply with the law (e.g., businesses, data/information brokers, government entities, etc.); definitions of "personal information" (e.g., name combined with SSN, driver's license or state ID, account numbers, etc.); what constitutes a breach (e.g., unauthorized acquisition of data); requirements for notice (e.g., timing or method of notice, who must be notified); and exemptions (e.g., for encrypted information). ❖

PPM Cyber Liability (eMD™) Insurance

In response to the increased public attention, federal and state regulations and potential liability arising from the disclosure of PHI, PPM recently announced, for the benefit of all PPM policyholders insured on January 1, 2015, the addition of Cyber Liability (eMD™) Insurance.

According to Brent Hodges, PPM's Vice-President of Underwriting, "the addition of Cyber Liability Insurance is being extended through a partnership with NAS Insurance, the leading provider of Cyber Liability Insurance to health care professionals in the United States." Standard coverage with $50,000 limits (including claims costs) will be provided to PPM policyholders for **no additional charge**. No underwriting is required and no deductible applies.*

First Party Coverage

PPM policyholders are protected from cyber risks involving a first party insured event and the reasonable and necessary costs and expenses incurred, including:

Privacy Breach Response Costs, Patient Notification Expenses, and Patient Support and Credit Monitoring Expenses – Includes all reasonable legal, public relations, advertising, IT forensic, call center, credit monitoring and postage expenses incurred by the insured as a result of a privacy breach.

Network Asset Protection – Coverage for all reasonable and necessary sums incurred to recover and/or replace data that is compromised, damaged, lost, erased or corrupted due to accidental damage or destruction of electronic media or computer hardware, administrative or operational mistakes in the handling of electronic data, or computer crime/attacks. Coverage also extends to business income loss and interruption expenses incurred as a result of a total or partial interruption of the insured's computer system caused by any of the above events.

Cyber Extortion – Coverage for extortion expenses and extortion monies incurred as a direct result of a credible cyber extortion threat.

Cyber Terrorism – Coverage for income loss and interruption expenses incurred as a result of total or partial interruption of the insured's computer system due to a cyber terrorism attack.

Third Party Coverage

PPM policyholders are also protected from liability claims brought by third parties, including:

Multimedia Liability – Coverage for third party claims alleging copyright/trademark infringement, libel/slander, advertising, plagiarism and personal injury. Covers both online and offline media.

Security & Privacy Liability – Coverage for third party claims alleging liability resulting from a security or privacy breach, including the failure to safeguard online and offline information, or the failure to prevent virus attacks, denial of service from attacks or the transmission of malicious code.

Privacy Regulatory Defense and Penalties – Coverage for defense costs and fines/penalties incurred in defending against regulatory investigations of privacy or security breaches.

Please feel free to contact your PPM sales or underwriting representative with any questions regarding PPM's Cyber Liability (eMD™) Insurance.

*Cyber Liability Insurance applies to data breaches occurring on or after the retroactive date of your PPM policy. Coverage is provided on a claims-made basis. Your PPM policy must be in force at the time the breach is reported to PPM. Entity Annual Aggregate Limits are based on the number of physician policyholders in entity. Higher limits of coverage may be purchased from NAS Insurance beyond the standard $50,000 limit. PPM's website, ppmrrg.com, will also provide useful cyber liability risk management resources via its partnership with NAS Insurance. For more information, please contact your PPM sales or underwriting representative.

PPM's Risk Management Seminars Certified for CME

Through a joint providership with Tulane University Health Sciences Center, PPM is pleased to announce that PPM's live risk management seminars have been designated for *AMA PRA Category 1 Credit*™. Tulane is an ACCME-accredited provider whose current status is Accreditation with Commendation. The *AMA PRA Category 1 Credit*™ system has become the CME standard for licensing boards and specialty organizations nationwide and is recognized by all U.S. jurisdictions. Thirty-nine states/territories will accept the AMA PRA certificate or the AMA approved PRA application as proof of having met the CME requirements for licensure, simplifying the medical re-licensure process. The approved AMA PRA application also meets Joint Commission CME reporting requirements in connection with a hospital's accreditation process.

"After several years of exploring joint providerships to find the right fit for PPM's risk management program, we are very excited to be able to offer PPM policyholders continuing medical education credit toward the prestigious American Medical Association Physician's Recognition Award," according to Brian Thomas, PPM's Director of Risk Management.

Since 1987, PPM has honed its anesthesia expertise using a substantial database of loss outcomes information based on our investigation of over 12,500 adverse anesthesia events. PPM utilizes this database to identify areas of risk, monitor developing loss trends, and provide practical, anesthesia-specific risk management advice and patient safety strategies. PPM policyholders also have exclusive access to timely and useful risk management resources at MyPPMrrg.com, including access to *Anesthesia & the Law*, PPM's risk management newsletter. ❖

Underwriter's Spotlight

Events that Trigger Medical Licensing Board Investigations

While all settlements of medical negligence litigation paid by professional liability insurance companies are reportable to both the National Practitioner Data Bank (NPDB) and state medical licensing boards, there are several other sources that might trigger a state medical board investigation. According to Patsy Kremer, PPM's Senior Underwriter, "PPM is passionately committed to protecting our policyholders' professional reputations and medical licenses. Becoming the subject of a medical board investigation is a serious matter that demands immediate attention and professional guidance and support." PPM strongly encourages our policyholders to contact our underwriting or claims departments in the event of any of the following:

- Patient complaint – either orally or in writing
- Hospital actions – suspension or non-renewal of privileges, sentinel events, root cause analysis or peer review of any incident
- Any action taken by any state medical board in which the PPM policyholder is licensed – e.g. if the PPM policyholder is licensed in multiple states, any action taken by a medical board in one of those states is typically reported to all states in which the PPM policyholder is licensed
- Actions by health insurance or managed care companies – e.g. if a health insurer revokes, suspends or non-renews a PPM policyholder's participation as a provider in the health insurer's network
- A "secret" source – e.g. anonymous complaints filed by hospital staff, patient family members, etc.

PPM reminds our policyholders that Medical Board Investigation Defense Expense coverage is available as an endorsement to your PPM policy. PPM's Medical Board Investigation Defense coverage provides a defense in the event the PPM policyholder becomes the subject of an investigation by a state authority responsible for the investigation of complaints regarding Medical or Osteopathic practice. PPM's Medical Board Investigation Defense coverage provides up to $25,000 for each investigation and up to $75,000 for all investigations first reported within any twelve (12) month period.

Please feel free to contact your PPM sales or underwriting representative to learn more about PPM's Medical Board Investigation Defense Expense coverage. ❖

PREFERRED PHYSICIANS MEDICAL RISK RETENTION GROUP, INC.
9000 West 67th Street
Shawnee Mission, KS 66202-3656

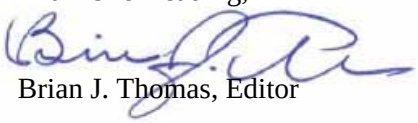
T 913.262.2585 • 800.562.5589
F 913.262.3633

NEWSLETTER EDITOR
Brian J. Thomas, JD
Senior Claims Attorney
Director of Risk Management

ANESTHESIA & the LAW
A Risk Management Newsletter
DECEMBER 2014 – ISSUE 40

In This Issue

Thanks for reading,



Brian J. Thomas, Editor