Volume 18, Number 3 · November 2015

Newsletter of Physicians Reimbursement Fund, Inc.

PRF NEWS

www.prfrrg.com · (415) 921-0498

Covering Practice and Risk Management Issues for Health Professionals

Is Your Patient Health Care Data Secure?

Take These Four Checklist Tests and Be Sure!

BY ADRIENNE M. LADD AND MARGARET S. LEONARD

Let's start with some simple questions: Does your practice use electronic health records? Third party billing services? Online portals or interactive websites where patients may enter their personal demographic and billing information? If the answer is "yes" to any of the above, you need to immediately ask yourself "Just how well is my patient data being protected?" And if you need a reason for why you should worry, the answer is equally simple: the risk of a security breach is high (and growing), and the potential penalties to you include extremely punitive fines, civil litigation, and even imprisonment.

"Depending on the nature of the breach, federal and state fines* for a single disclosure *of a patient's protected personal health information could reach as high as $1.5 million."

According to the U.S. Department of Health and Human Services, one in 10 Americans has been affected by a large health data breach. In 2013, one out of five health care organizations experienced a security breach, and health care data breaches accounted for 44 percent of all breaches – the first time the health care sector topped this list. These breaches were attributed most frequently to employee negligence, computer malware and viruses, digital intrusion/theft, and physical intrusion/theft.

Depending on the nature of the breach, federal and state fines *for a single disclosure* of a patient's protected personal health information could reach as high as $1.5 million. This doesn't even take into account legal fees, credit monitoring fees, IT recovery fees, or costs associated with reputation damage.

The financial impact to medical office practices is summarized in the table on the next page.

As you begin thinking about the protection of your patient data within your office, there are four specific areas of your practice to consider for HIPAA compliance and data security:

- IT security and risk considerations
- Electronic Health Record (EHR) system security
- HIPAA-related office policies and procedures
- Business associate (BA) agreements

IT Security and Risk Considerations

Reviewing your hardware and software infrastructure (servers, personal computers, and internet virus protection) is a key component of an office security and risk assessment. What follows is a quick checklist for review.

- ✓ Is your hardware/software supported by a professional IT management company?
- ✓ Does this support include computer/server installation, data backup, system access logs, intrusion detection monitoring, and software updates including antivirus protection?
- ✓ Are your local computer/servers located in secure, locked locations?
- ✓ Is your office computer hardware susceptible to theft during office hours or after office hours?
- ✓ Beyond having an alarm system for after-hours security, does the staff provide continuous visual security for office systems during business hours?
- ✓ Do your office computers require security passwords?

(continued on page 2)

Inside PRF News

Is Your Data Secure? *(continued from page 1)*

- ✓ Is each computer and server password protected?
- ✓ Are your computer passwords viewable by visitors?
- ✓ Are the files and hard drives on your office computer desktops encrypted?
- ✓ Are your office servers protected from accidental activation of fire suppression systems?
- ✓ Does your office local server provide a single point of data backup? (If so consider offsite data backup.)
- ✓ Is your office email secure (encrypted) when sending Personal Health Information (PHI)?
- ✓ Does your email provider provide encryption capability for transmission of patient PHI?
- ✓ Is your staff adequately trained in encryption procedures?
- ✓ Does your employee handbook indicate that all PHI sent via email will be encrypted?
- ✓ Does your office have a procedure to monitor that policies and procedures are followed?
- ✓ If your office website allows patients to enter their information or provide billing information, is that information encrypted?

EHR Security

Electronic Health Record system security considerations are frequently overlooked during implementation in an office practice. Here is a best practices checklist of specific EHR office policies and procedures for your office:

- ✓ Does your office have defined and monitored EHR access? Clinical patient information and billing information are prime considerations for access by office staff. Unauthorized access means inappropriate review or viewing of patient medical information without a direct need for diagnosis, treatment, or other lawful use.
- ✓ Are procedures in place for routine auditing of EHR access logs? Routine monitoring of EHR access logs is required to insure that PHI is appropriately accessed by staff.
- ✓ Are consequences for unapproved access to PHI described? Informing office staff at the start of employment and during routine performance reviews of office policy regarding PHI access is a best practice.
- ✓ Is there an office policy and procedure addressing both planned and unplanned termination of staff system access? Often system access is controlled by an offsite IT vendor. Prompt notification of staff termination (planned and unplanned) is critical to protection of office PHI.
- ✓ Does your office provide security for office computers and computer access?
- ✓ Are computers and office servers secured (locked doors) during non-office hours, and is access monitored by staff during working hours of the office?
- ✓ Is there a policy and procedure addressing system passwords (format, password change policy, password security)? An office policy requiring password changes often meets resistance by office staff but is a best practice for IT security/PHI security. An office policy for IT configuration regarding password complexity and password protection is routine for EHR systems but easily overlooked.
- ✓ Are there policies and procedures addressing EHR data recovery and restoration? The need for data recovery and restoration may occur as a result of a disaster (e.g., fire, flood, earthquake, temporary building disruption) or disruption of EHR vendor applications. Having offsite data storage with a reputable IT vendor will facilitate office data recovery and restoration. Your office will benefit from having well-documented procedures for staff notification, office down time, and patient notification.

Table 1: Financial Impact to Medical Office Practices

Entity	Violation	Fine, Jail Time
HIPAA Civil Penalties	HIPAA unknowingly violated	$100-$50,000
	Due to reasonable cause, not due to willful neglect	$1,000-$50,000
	Due to willful neglect, corrected within 30 days of notice	$10,000-$50,000
HIPAA Criminal Penalties	Violation due to willful neglect, not corrected within 30 days of notice	$50,000, 1 year jail
	Violation committed through deception	$100,000, 5 years jail
	Sale or transfer of health information for profit or any personal gain or intent to harm	$250,000, 10 years jail
CA State Laws	Apply to individuals as well as health care providers and business associates	Up to $250,000, 10 years in jail

HIPAA Compliance

HIPAA-related office policies and procedures frequently overlook specific items. Here is a checklist of specific HIPAA-related items for inclusion in your office policies and procedures:

- ✓ Does your employee handbook adequately address HIPAA/PHI education?
- ✓ Is the frequency of HIPAA training (for new employees and continual training) described?
- ✓ Are employees required to pass a test demonstrating HIPAA knowledge upon employment?
- ✓ Are employees required to pass a test demonstrating HIPAA knowledge at defined intervals of employment?
- ✓ Are there clearly-defined guidelines for employee social media use? Social media office policy considerations should note that information obtained through your work is confidential, posting patient information without authorization is a violation of the patient's right to privacy and confidentiality, and de-identification

(continued on page 4)

STAY SAFE ONLINE

The National Cyber Security Alliance offers additional tools and resources on cyber security. For more information visit https://www.staysafeonline.org/. ■

How Emotions Inform Patient Satisfaction

BY KIMBERLEE A. SOREM, MD, MA

Patients' satisfaction depends on their ability to understand both the objective aspects of their care as well as their subjective emotional and psychological experiences. Through increased understanding of patient emotions, physicians can help with this process. Thoughtful physician communication that respects these complex emotions is not only in the best interest of the patient, it also mitigates medical-legal risks.

We can begin to address this complexity by anticipating that the some of the following emotional components will likely accompany and color our discussion of medical treatment plans, options, and outcomes with patients:

1. Respecting **expectations** (worries)
2. Understanding potential **benefits** (hopes)
3. Assessing **risk** (fears)
4. Managing **disappointments** (frustrations)
5. Addressing **adverse outcomes** (anger)

Expectations: Outcome expectations form in response to a patient's anxieties. Patients frequently are worried that their disease or condition has the potential to cause them yet more harm or suffering. Their expectation is that the medical plan will prevent that from happening and may lead to an overly optimistic belief about the consequences of receiving treatment. The belief that treatment will always lead to improvement is a good example. Although complex medical technologies may dazzle patients, this very excitement may interfere with their ability to understand that medical innovations cannot always produce the desired result.

What to do:

- Directly discuss expectations with the patient.
- Ask what he/she bases these expectations on. Try to understand their emotional thought process.
- Empathize with the *worry* that their expectations may not be met and they may experience additional injury or suffering.

Benefits: Assessing potential benefits goes beyond simply stating measurable medical and technical data. It also requires an emotion-mediated internal evaluation; i.e., it involves contending with the patient's hopes. And hope, as we know, can both protect and distort. While understanding what is possible to achieve, the patient must also temper this hope with the known facts about the scope and limitations of the benefits. Physicians, in turn, must address their patients' hopes by accurately providing the information about what we do and do not factually know about the potential benefits of a treatment or procedure.

What to do:

- Directly discuss the known data and the theoretical possibilities.
- Explain that the benefits may be partial or temporary.
- Empathize with the *hope* that the benefit is realized.

Risks: Assessing risk also goes beyond an understanding of measured outcomes and published data. It also involves emotion-mediated internal evaluations. The emotion to contend with here is fear. While fear may make a person sober and clear-eyed, it may also distort risks and impair judgment. Again we need to help patients to manage fears and expectations by providing not only the known facts but also the unknown or potential areas of concern. We cannot know all risks, and patients need to understand that. They have to trust that we have disclosed as much as we know, and that we, too, have a healthy respect for the risks that they take with us.

What to do:

- Directly discuss known data and unknown possibilities.
- Explain how you attempt to minimize risk.
- Explain that both action and inaction have risks.
- Empathize with the *fear* that the risk is too great.

Disappointments: We cannot protect patients from certain disappointments (and we cannot protect ourselves from disappointed patients). Disappointments may result from a partial or unanticipated response to medical treatment. Some patients process disappointment better than others, but nearly all feel frustration with having to manage this at all. Our ability to empathize with these frustrations allows us to help them strategize about the next steps, which therapies to try, or when to stop trying.

What to do:

- Directly discuss their disappointments without minimizing the effect that the disappointments have had.
- Explain what happened without being defensive.
- Explain what might be expected to change or not to change in the future.
- Empathize with the *frustration* that disappointments cause.

Adverse outcomes: Any time a patient suffers a medical or iatrogenic injury, it is an adverse outcome. Yet an adverse outcome may or may not be the result of medical error and not all medical errors result in an adverse outcome. In addressing adverse outcomes the physician should recognize that helping a patient can mean dealing with the patient's reaction to injury or even to medical error that did not result in injury (but can still produce feelings of anger). In doing so, physicians should try to help patients emotionally process whatever damage or loss he/she may feel.

One way physicians can respond to medical error is to apologize. Apologies—statements that acknowledge an error and its consequences, as well as take responsibility and communicate regret for having caused harm—can decrease blame, decrease anger, increase trust, and improve relationships. Although the fears of potential litigation are the most commonly cited barrier to apologizing after medical error, the link between litigation risk and apology is

(continued on page 4)

"Although complex medical technologies may dazzle patients, this very excitement may interfere with their ability to understand that medical innovations cannot always produce the desired result."

Four Checklist Tests *(continued from page 2)*

of PHI requires removal of all 18 PHI identifiers, which includes "Any other unique identifying number, code, or characteristic" (e.g., photo of a wound; description of a patient's condition).

- ✓ Does your employee handbook adequately address HIPAA/PHI information transmission, destruction, and data breach notification?
- ✓ Do your office procedures address the security of paper documents containing PHI?
- ✓ Are paper documents containing PHI adequately secured (in secured storage or protected from theft or viewing) within the office during office hours?
- ✓ Are there policies and procedures for the secure destruction of paper documents containing PHI?
- ✓ Do your office procedures address the security of facsimile transmissions containing PHI?
- ✓ Does your office policy address procedures required to insure PHI is transmitted to the correct recipient?
- ✓ Does your office policy address notification procedures in the event of incorrect receipt of PHI?
- ✓ Do your office procedures address notification by staff about a data breach (e.g., transmission to other external entities, accidental loss of office PHI)?

Business Associate Agreements

A Business Associate is a person or organization that performs functions or provides services that involve the use or disclosure of individually identifiable health information. For example, PRF is a Business Associate to each of its Insureds.

Every health care provider who transmits health information electronically in connection with certain transactions is a Covered Entity. Common transactions include claims, benefit eligibility inquiries, and referral authorization requests.

Business Associate functions or activities on behalf of a Covered Entity include claims processing, data analysis, utilization review, and billing. Business Associate services to a Covered Entity are limited to legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services. Individuals and organizations are not considered Business Associates if their functions or services do not involve the use or disclosure of PHI, and where any access to PHI would be incidental, if at all.

A checklist of items sometimes overlooked in medical office BA agreements follows:

- ✓ Does your BA agreement outline when and how the BA may disclose PHI?
- ✓ Are PHI conditions of use by the BA clearly outlined?
- ✓ Are the exclusions identified so that the BA will not disclose PHI except as permitted?
- ✓ Does the language outline how the BA implements HIPAA safeguards for electronic PHI?
- ✓ Does the agreement state that the BA is to report to the Covered Entity any use or disclosure of PHI not covered by contract?
- ✓ In the agreement, does it say that the BA must return or destroy any PHI as covered by the contract at the conclusion of the contract?

Performing your own security and risk assessment may help you avoid disastrous compliance consequences. We strongly urge you to use these checklists to expose risks you were not aware existed. In the end they will provide you with piece of mind regarding the security of PHI within your practice. ■

Margaret S. Leonard is a Consultant and Adrienne M. Ladd is a Delivery Leader with Freed Associates, a California-based firm providing consulting services for health plans, hospitals, physician practice groups, life sciences and related health care organizations.

Emotions Inform Patient Satisfaction *(continued from page 3)*

weak. In fact, apologizing may have important effects on both the person offering it and the recipient.

What to do:

- ➤ Recognize that error/injury has occurred.
- ➤ Accept responsibility for causing harm without acknowledging fault.
- ➤ Directly disclose the facts: what is known and what is unknown.
- ➤ Apologize and communicate sincere regret.

In summary, the relationship between patient and physician is a complex and intimate one. As with all relationships, emotions can induce a positive a sense of wellbeing or impair judgment. In our role as physicians, we should seek to respect patient emotions and to understand how to address them. In so doing we may be able to improve communication, enhance patient satisfaction and reduce medico-legal risks. ■

Dr. Sorem is board-certified in OB/Gyn with subspecialty board certification in Maternal Fetal Medicine. She also has a graduate degree in counseling psychology from the Wright Institute in Berkeley and runs a private psychotherapy and consultation practice, concentrating on patients who have suffered pregnancy losses or who have complex psychological issues including management of medications in pregnancy.

PRF NEWS Volume 18, Number 3 · November 2015
Covering Practice and Risk Management Issues for Health Professionals
Stephen Scheifele, MD, *Executive Editor*
Robert D. Nachtigall, MD, *Editor*

Physicians Reimbursement Fund, Inc.
711 Van Ness Avenue, Suite 430
San Francisco, CA 94102
(415) 921-0498 - voice
(415) 921-7862 - fax
Andrea@PRFrrg.com • www.PRFrrg.com

Andrea McArtor, *Executive Director*
Soad Kader, *Director of Membership*
Shannon Gates, Esq., *Claims Adminstrator*