# HPSO *Risk Advisor*
Healthcare Providers Service Organization℠

# Protect Your Organization Against Data Security Breaches

Consider the following examples of data security breaches and ask yourself whether your organization may be vulnerable to similar scenarios:

- A hacker breaks into a rehabilitation facility's computerized record system, exposing patients' protected medical information.
- A disgruntled employee of a counseling practice copies financial data, including social security and credit card numbers.
- A community health clinic administrator loses a laptop computer containing identifiable patient billing information.
- A vendor engaged to digitize a diagnostic center's paper files makes an error, potentially corrupting thousands of individual patient records.

Each of the above examples illustrates the risks of data security breaches in the healthcare industry. Analysis of Privacy Rights Clearinghouse findings indicates that 11 percent of all reported incidents of privacy breach between February 2005 and February 2007 involved healthcare entities.[1]

This article offers strategies designed to prevent data breaches from occurring and to reduce potential liability for data-related losses via contractual risk transfer and insurance. It also includes guidelines for mitigating damage and complying with legal requirements in the event that confidential information is compromised.

## Preventive Strategies

A data security breach can have devastating consequences for healthcare organizations as well as patients or clients. To reduce the likelihood of such an occurrence, incorporate the following basic strategies into your data security program:

**Utilize an encryption system.** Password protection of your organization's computers is necessary but not sufficient to secure patient privacy. Confidential data should be encrypted – i.e., readable only to those with

the proper electronic "key." Under many breach notification laws, the theft or loss of encrypted data does not trigger the duty to



notify. However, the loss of password protected unencrypted information does require notification.

**Place controls on data storage and access.** Clear, auditable and enforceable policies controlling access to your information system must be implemented to protect resources and data from misuse by insiders, including employees, vendors and customers. Firewalls and anti-virus systems can prevent unauthorized access to or corruption of data by outsiders.

**Regulate use of portable devices and storage media.** According to the Privacy Rights Clearinghouse, 40 percent of the security breaches reported by medical centers in 2006 involved laptop theft.[2] Thus, formal written procedures governing the use, transport and storage of laptops, disks and other portable equipment should be established and enforced. Users must be reminded that portable computers are prime targets for thieves, and that the convenience of downloading patient or client data to a laptop must be balanced against the possibility of loss or theft.

**Carefully dispose of old equipment and outdated records.** Establish policies to ensure that only current, relevant records are retained. Purge digital patient or client records on a regular basis, and document the destruction. An effective means of addressing the data-exposure risk associated with

obsolete computers and storage media is to "scrub" old equipment of all contents before disposing of it.

**Keep a backup set of records off-site.** By retaining an extra set of records at a separate location, you can prevent large-scale data loss or corruption from a computer virus or other system breach.

## Risk Transfer and Insurance

An estimated 30 to 40 percent of all data confidentiality violations involve contracted third parties, including call centers, data center operators, IT consultants and other service providers.[3] For this reason, contractual risk transfer constitutes a key element of any data security program. Whenever you entrust sensitive or non-public personal information to a third party, require signed acknowledgment of the following contractual protections:

- an agreement regarding access to and appropriate use of your information and networks, including compliance with your practice's information security standards
- indemnification/hold harmless agreements for all costs arising from breaches of the third party or the wrongful use of confidential data by their employees

Such business associate agreements must comply with the requirements set forth in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) [Public Law 104-191], the Privacy Rule and the Security Rule, 45 CFR Parts 160, 162 and 164, subparts A and E. When drafting contracts, work with an attorney who has expertise in the complex legal issues surrounding patient or client privacy, data security and HIPAA regulations.

The full range of damages associated with a data security breach may not be covered by your healthcare business's general and professional liability policies. Specialized insurance products are available to address

technology-related risks, and many healthcare providers and organizations are incorporating these products into their overall insurance program. Consult your insurance advisor about closing any gaps in your coverage.

### Post-breach Response

If you suspect your information system has been targeted and patient or client information exposed, a rapid assessment and mitigation of damage is imperative, as outlined below: Evaluate the severity and scope of the incident. If a laptop computer or other portable device is lost or stolen, identify the data that may have been exposed, and determine whether these materials are encrypted or protected by password. Consider engaging forensic experts to define the scope of the problem. In addition, if the possibility of identify theft or other criminal action is present, inform appropriate law enforcement agencies of the situation.

**Notify potentially affected patients or clients.** Most states now mandate notification of customers whose confidential data may have been exposed. Healthcare businesses that have experienced a security breach also may be required to pay for credit monitoring services for potential victims. Federal law specifically addresses healthcare providers, requiring them to warn affected persons of the risk of identity theft and fraud within a stipulated timeframe. Consult with legal counsel regarding applicable notification laws.

**Go beyond minimal legal compliance.** Because the public expects healthcare providers and healthcare practices to safeguard personal, medical and financial information, a data breach can tarnish your facility's reputation. You can begin to repair trust and reduce follow-up losses by offering credit monitoring services and identity theft case management to affected patients or clients. A sound communication strategy featuring regular, comprehensive updates also can help mitigate the harm of lost or stolen data.

In a computer-dependent world, the risks associated with client/patient data exposure, theft or alteration cannot be taken lightly. By establishing an effective data security program and preparing a post-incident response plan, you can help protect both your patients or clients and your own organization against the occurrence and potential consequences of security breaches.

### References

1. "Chronology of Data Breaches 2006: Analysis," available for viewing at http://www.privacyrights.org/ar/DataBreaches2006 Analysis.htm
2. Ibid.
3. Ponemon Institute, "2007 Annual Study: Cost of a Data Breach," November 2007, p. 6.

### Other Resources

• The Federal Trade Commission's identity theft Web site, at http://www.ftc.gov/bcp/edu/microsites/idtheft/, contains information, tools and additional links relating to data security.
• The Privacy Rights Clearinghouse Web site, at www.privacyrights. org, offers a range of resources for understanding, preventing and mitigating data security breaches, including a frequently updated "Chronology of Data Breaches.

## Staff Credentialing: These Fundamental Principles Can Help Reduce Risk

**T**he history of malpractice litigation over the last decade demonstrates that all allied healthcare businesses are vulnerable to professional liability claims, including allegations that involve independent practitioners, mid-level providers or other healthcare providers working for a healthcare practice. Therefore, a sound credentialing program is not only essential to maintaining quality and protecting your patients from harm, but may also safeguard your healthcare practice against vicarious liability claims.

Credentialing is the process of assessing and validating the qualifications and competence of a licensed practitioner to offer services in a healthcare setting. It involves deciding whether the applicant is qualified to provide patient care within your practice, and what specific clinical privileges should be granted. Credentialing is a critical element of every healthcare practice's enterprise-wide risk management strategy.

The fundamental credentialing guidelines in this article can be applied whether you are developing, evaluating or revising your facility's policies and procedures.

### Researching Standards

To function effectively, your credentialing mechanism must reflect your range of services, jurisdiction, and practitioner population. Adopting boilerplate policies from other facilities may result in unwise decisions and unexpected liability exposure.

To view a checklist designed to help your organization comply with established guidelines for the credentialing process, please go to **www.hpso.com/staffchecklist**.

Because the credentialing process is driven primarily by accreditation standards, as well as federal and state law, you should first become conversant with the provisions that apply to your particular healthcare setting. For example, the federal mandates for verification of license and qualifications under the Medicare Conditions of Participation (which can be accessed at www.cms.hhs.gov/CFCsAndCoPs/) apply to home health agencies and outpatient rehabilitation facilities, among other allied healthcare settings.

## Establishing Criteria

After identifying and reviewing the credentialing mandates applicable to your practice, you can then establish standards reflecting the appropriate competence level for various procedures in your facility. If you have several practitioners employed at your healthcare practice, you may want to consider having a clinical appointment committee charged with defining qualifying criteria in such areas as:

- healthcare provider's certification/registration
- board certification
- education
- licensing requirements
- medical professional liability claim history
- professional experience
- references
- training

These criteria should be set forth in your business's governance documents – including staff rules and regulations, as well as clinical policies and procedures – to ensure their systematic and consistent application. In addition, you will want to approve the credentialing process and oversee its implementation.

## Privileging Clinical Procedures

After you and/or your clinical appointment committee has deemed a practitioner qualified to practice within your organization, you must then determine his or her scope of practice and supervisory requirements. Because laws governing clinical scope of practice and extent of supervision vary among states and across practice settings, it is essential to obtain input from competent legal counsel when making credentialing decisions.

Before granting privileges to perform a proposed clinical procedure, it is prudent to consider a variety of factors, rather than focusing exclusively on marketplace pressures and opportunities. If a procedure is identified as high risk, it must be scrutinized to determine whether benefits outweigh hazards.

The following questions are integral to the privileging process:

- What does the peer-reviewed literature say about the procedure or treatment and the relevant standard of care?
- What complications are most commonly associated with the procedure or treatment?
- How can your facility best protect patients against these possible complications?
- Have you, your facility leaders, or administrators documented your understanding of the risks associated with the procedure or treatment?
- Can your practice's infrastructure, clinical staff, currently available equipment and training programs adequately support providers seeking to perform the procedure or treatment?
- Does the procedure fit within your practice's current mission and future plans?

Clinical privileges must reflect the scope of your facility's licensure requirements, as well as its human, technical and financial resources. A sound privileging process is fundamental to maintaining quality standards and fostering careful and controlled growth.

## Reducing Exposure

Many healthcare facilities rely on the credentialing system of their larger affiliated institutions. If such an information-sharing system is available to your facility, document the arrangement in a written contract, and verify that the records, protocols, and rules and regulations of both organizations reflect this relationship. In addition, confidentiality agreements should be executed between the two facilities and the individuals charged with performing credentialing procedures. A detailed written agreement can prevent future disputes over the release of information.

The most effective way to reduce your exposure related to negligent credentialing claims is to implement protocols that clarify administrative responsibilities and ensure conformity with federal and state licensure laws, regulations and standards.

Your protocols should reinforce the following fundamental principles:

- Clinical assignments are granted or denied based upon objective, carefully documented institutional criteria.
- Practice rules, regulations and standards are applied equitably to all applicants.
- Quality outcome data and patient information used in the process are treated with utmost confidentiality.
- All clinical assignment decisions are communicated to the applicant by letter.
- Credentialing and clinical assignments are carefully delineated.
- Decisions are documented in the applicant's file, which is maintained in a secure location.

The credentialing and clinical assignment process is at the heart of healthcare risk management. By periodically reviewing and refining your credentialing methods and policies, you can help improve patient safety, minimize the consequences of provider malpractice allegations and better manage your organization's future.

# Telephone and E-mail Communication: Securing Patient Privacy

While telephone and e-mail facilitate contact with patients, they also may jeopardize privacy. To safeguard patients' protected health information (PHI), it is necessary to develop and implement written policies addressing the appropriate and secure use of these basic communication tools. Let's look at strategies to reduce liability exposure associated with patient interaction via telephone and e-mail.

## Parameters of Use

Telephone and electronic communication is most suitable for brief exchanges involving minimally sensitive information, such as appointment reminders, benefit and billing inquiries, non-urgent medical advice, and normal laboratory results and follow-up.

The consent form presented at the initial patient visit should outline the expectations, risks and limitations of your organization's e-mail and telephone advice practices. Once signed, the authorization should be inserted in or attached to the patient care record. Patients must provide additional written authorization to receive and exchange PHI electronically and/or by telephone.

## Security Guidelines

The two key risk management principles when communicating electronically or by telephone are to ensure security of transmitted information and privacy of content. The following measures can help staff members reduce e-mail risks:

✓ Avoid patient identifiers in the subject heading, such as the patient's name or medical record number.

✓ Include a privacy notice with all e-mails stating that the communication is confidential and contains information protected by the provider-patient privilege.

✓ Limit unsecured messaging to notification of services, such as educational programs and community health clinic offerings.

✓ Never send blind copies or group e-mails where other names are visible to recipients.

✓ Rely on a centralized patient e-mail database to prevent distribution errors and duplications, and do not use personal e-mail accounts.

✓ Retain the original e-mail message in the electronic patient care record when replying, and include a confirmation receipt request.

✓ Transmit through an approved and secure server, using tested encryption technology.

Security provisions when communicating by telephone include the following:

✓ Designate a telephone conversation area located away from patient care or waiting areas to ensure privacy.

✓ Use landlines when possible, and inform patients that cellular telephone messages may be intercepted.

✓ Never leave sensitive information—such as test results or medical advice—on an answering machine, in a voicemail message.

✓ Update patient telephone numbers (as well as e-mail addresses) on a regular basis, or with an answering service.

Security and privacy policies should adhere to the parameters of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule, which is available at http://www.cms.hhs.gov/SecurityStandard/02_Regulations.asp# TopOfPage

## Staff Training and Monitoring

Telephone and e-mail exchanges tend to be less systematic than face-to-face interviews, increasing the possibility of misdiagnosis. It is therefore necessary to train staff in interviewing techniques, as well as selecting and applying advice protocols. Training should focus on eliciting information to rule out potentially hidden conditions, especially those related to the head, chest and respiratory system.

By observing telephone and electronic interactions through your quality improvement program, you can ensure that staff members are routinely capturing the following minimum clinical data:

✓ aggravating/relieving factors

✓ allergies

✓ current medication use

✓ pregnancy status

✓ previous medical and surgical history

✓ recent injury, illness or infection

✓ psycho-social history

✓ symptoms of chief complaint and history of onset

All patient interactions involving description of symptoms should be conducted by clinical professionals, with physician supervision, as appropriate.

## Advice Protocols

Most patient telephone calls and an increasing number of e-mails result in self-care treatment within the parameters of advice protocols. The goal of such protocols is to enhance clinicians' ability to gather accurate information and provide safe, effective and consistent treatment recommendations that incorporate current medical knowledge.

The following safeguards can help limit liability linked to advice protocols:

✓ Advise callers to seek medical attention if symptoms worsen or fail to improve within 24 hours, and refer them to an emergency department when indicated.

✓ Establish parameters for symptoms necessitating a return call by the patient and/or healthcare provider.

✓ Review protocols annually and maintain discontinued ones in a secure location.

✓ Securely fax or e-mail patients' health information sheet following any protocol-based discussion.

✓ Use a checklist format for protocols to enable thorough, consistent documentation.

## Documentation

Electronic patient communication is subject to the same documentation and retention requirements as other media. E-mails can easily be attached to an electronic medical record. If your practice relies upon paper records, print out e-mails and file them in the record as progress notes.

Unlike self-documented e-mails, telephone messages must be written down after the discussion and placed in the progress notes section of the patient care record. Preprinted telephone logs should be used to document:

✓ patient's name and age

✓ date and time of correspondence

✓ identity of the caller/sender when different from the patient's

✓ chief complaint or concern

✓ brief history and assessment

✓ advice protocol used

✓ name and signature of responding staff member

✓ necessary follow-up, such as a required return call

In addition, develop a documentation format for telephone responses to e-mails and e-mail responses to telephone discussions.

### Resources

• E-mail as a Provider-Patient Electronic Communication Medium and Its Impact on the Electronic Record, prepared by the American Health Information Management Association at www.ahima.org. (Click on HIM Resources, then Practice Briefs, then Privacy, Confidentiality, and Security.)

• "Risks and Strategies Related to Effective Telephone Communication," part of the Physician Office Risk Management Tool Kit. Available from the American Society for Healthcare Risk Management at www.ashrm.org.

**CNA**