Protecting Your Practice from Unauthorized Email Disclosures

By: Jennifer Kirschenbaum, Esq.
Jesse Kirschenbaum

Sure email is a great way to keep in touch; it's convenient, fast, accessible and documented. In fact, email is so simple it's easy to forget certain precautions you might take if you were communicating with a patient via traditional written communication or on the phone. Now that more and more patients are internet savvy, more and more patients are demanding their physicians answer emails. A main concern with the increase of email communications is that oftentimes people are much more casual in their writing and the formalities put in place to protect patient confidentiality in the office may be forgotten or ignored.

Disclosure Led Investigation

Just such an example recently happened to a practitioner when the girlfriend of a quasi-celebrity patient sent an email in the middle of the night stating that the patient was unavailable and there was an emergency situation requiring the disclosure of medications the patient was taking. The practitioner was familiar with the patient's girlfriend; she had accompanied the patient to several visits and was present in the exam room for sensitive discussions. In the email received, the girlfriend explained that the patient was held against his will at a medical facility and was unreachable for consent. The practitioner, trying to protect the welfare of the patient, contacted the facility and confirmed the patient was indeed unavailable to give consent. After confirming the representations in the email, the practitioner disclosed the medications prescribed for the patient to the girlfriend, who then, inadvertently, leaked the information to the media. After the fact, it was confirmed there was an emergency situation and the patient did benefit from the disclosure; however, the patient, feeling betrayed and harmed by his practitioner's disclosure, filed a complaint claiming a Health Insurance Portability and Accountability Act (HIPAA) violation with the Office of Civil Rights, the government agency responsible for receiving and investigating HIPAA complaints. An investigation was commenced against the practitioner for an unauthorized disclosure. The investigation found that since the girlfriend was not listed on his HIPAA consent form for authorized access as a third party, an unauthorized disclosure had, in fact, been made and in this instance "emergency" was not a valid exception.

The aftermath of the disclosure for the practitioner was costly: emotionally and financially, as the practitioner endured a lengthy, nerve-racking investigation resulting in sanctions and high legal fees. The good news for the practitioner was no civil lawsuit was commenced, the fees sanctioned were limited and the practitioner was not referred to the Office of Professional Medical Conduct for a licensure investigation, all of which were available options after the breach.

The above is one example of why it is imperative to make sure that as your patients demand greater access to you via the internet, you and your practice respond by implementing greater precautions to protect against potential breaches. Such precautions include adopting, implementing and making your patients aware of the practice's security policy governing electronic individually identifiable health information (E-PHI) disclosures.

Adopting the Right Security Policy for Your Practice

For guidance on a proper policy limiting unauthorized disclosures the government has included in the HIPAA requirements/suggestions that all practitioners creating or receiving E-PHI adopt, such as administrative, physical and technical safeguards outlined below.

1. Administrative Safeguards: The administrative safeguards adopted should provide for security measures to protect E-PHI and a system to assess potential risks for E-PHI held by the practice. Also, the practice should regularly test and update security measures to ensure the confidentiality, integrity and availability of all E-PHI the practice creates, receives, maintains or transmits, to protect against those identified threats or hazards. Finally, with any policy, sanctions for potential violations should be promulgated for the practice staff to be aware of the cost of noncompliance, which may include termination.

2. Technical Safeguards: The technical safeguards implemented should include limiting physical access to E-PHI, while ensuring that properly authorized access is allowed. To accomplish same the practice should control and validate a person's access limited to their role and function by, for instance, assigning a unique name and/or number for identifying and tracking user identity and ensuring all workstations are programmed to terminate any electronic session after a predetermined time of inactivity.

3. Physical Safeguards: The physical safeguards implemented should include protection for the practice location and its equipment from unauthorized physical access, tampering and theft by password protecting all E-PHI access points and ensuring that all access to E-PHI is limited to authorized users. Additionally, all E-PHI should be destroyed in a manner not recoverable before it is thrown out.

The safeguards outlined above focus on protecting E-PHI from unauthorized access, whereas the above example evinces a knowing disclosure that was not authorized by either the practice's privacy policy or HIPAA, which is why an effective security policy requires more than adopting written procedures for protecting access to E-PHI. An effective security policy requires integration with the rest of the practice's policies and procedures, and also that your patients are aware of the practice's policies and procedures so that if a disclosure is prohibited under the practice's privacy policies, you and your staff remain aware the same disclosure is also prohibited when communicating online with E-PHI.

Implementing the Right Security Policy for Your Practice

The best way to ensure your practice is protected from unauthorized disclosures is by properly utilizing your security policy by incorporating its protections into the practice's day-to-day operations. One of the most effective ways to accomplish this is for your practice to designate a security officer who will be responsible for implementing and maintaining the policy and ensuring that all staff members of the practice adhere to the policy. It is recommended that each employee acknowledge receipt and review of any practice policy at least annually, and that a documented record of the employee's understanding of the policy be maintained on file.

Notifying Your Patients of Your Security Policy

In addition to adopting and implementing your security policy with practice staff, it is important that the practice take affirmative steps to notify patients of the practice's security policy. Easy ways to do this include providing patients with a copy of the practice's security policy along with the practice's privacy policy and posting the security policy in a visible location in the practice waiting room. Making the security policy available and including rules governing email communications will establish a standard for patient expectations. By managing patient expectations you lower your risk of facing a situation similar to the one we discussed above.

In sum, by adopting, implementing and promulgating an effective security policy, you will protect your practice from unauthorized disclosures by establishing set parameters governing email communications and effectively managing patient expectations.

If your practice does not have a security policy, visit www.kirschenbaumesq.com/healthcareorder.htm or Jennifer@Kirschenbaumesq.com.

CIGNA: Compensation for CEO Decreased by 50% in 2008

Overall compensation for Cigna CEO Edward Hanway decreased by 50% to $11.4 million in 2008 because of a decline in his performance bonus linked with the company stock price. In 2008, his salary increased by 3% to about $1.1 million, but his bonus decreased by 63% to about $6.7 million. Cigna said that bonus involves work performed from 2005 to 2007 and that Hanway and other top company officials did receive a performance bonus for 2008.

(Chicago Tribune)

State Legislature Enacts Budget Reduction Measure without New Taxes or Fees

(continued from page 1)

• Over $600 million in cuts to programs in 134 areas including health care, higher education, transportation and children and family services, including:

(1.) 12.5 % cut to remaining balances of local assistance programs and HCRA-supported programs such as graduate medical education, ambulatory care training program, physician loan repayment program, and health care worker recruitment and retention;

(2.) 5 % cut to operating aid for SUNY, CUNY and community colleges;

(3.) 5.4 % cut to the Office of Mental Retardation and Developmental Disabilities;

(4.) $107 million in various health care actions including freezing trend factors and delaying HEAL payments.

The agreed upon DRP also includes several one-shot or non-recurring sweeps including:

(1.) $200 million from the Battery Park City Authority,

(2.) $90 million from the Regional Greenhouse Gas Initiative;

(3.) $10 million from the Environmental Protection Fund; and

(4.) $26 million from the Dormitory Authority.

The Governor also agreed to $485 million in agency cuts. Furthermore, the Legislature passed a bill instituting a new Tier V in the New York State and Local Retirement System for public employees entering the system on or after January 1, 2010.

With a sizable Budget gap for this and the next fiscal year still outstanding, the Legislature is likely to consider further cost-cutting and/or revenue raising measures when they return to Albany for the 2010 Legislative Session next month.