A webinar series that keeps you in the know
Brought to you by Progressive eSupport

HIPAA

Nancy Stephens
Progressive Huddle
March 23, 2015

In this Webinar…

- Overview of HIPAA leadership
- Unacceptable uses of information or electronic devices
- Definition of a Breach
- HIPAA and cash paying patients
- HIPAA Risk Assessment Tool Kit

Overview

- **Provide Leadership**
  - HIPAA requires covered providers to designate both a privacy and a security officer on their staff.
  - Your leadership and constant emphasizing the importance of protecting patient health information is vital to your privacy and security activities.

Overview

- **Document your process, findings, and actions**
  - Documentation shows why and where you have security measures in place, how you created them, and what you do to monitor them. Create a paper or electronic folder for your records.

Overview

- **Conduct Security Risk Analysis or use our Risk Assessment Tool**
  - Conduct a security risk analysis (or reassessment if you already conducted an initial risk analysis) that compares your current security measures to what is legally and pragmatically required to safeguard patient health information.

Unacceptable Uses of EHI

- Example of some policy guidelines to have in place that outline the following activities as strictly prohibited, with no exceptions for System and Network Activities:
  - Accessing data, a server or an account for any purpose other than conducting ASC business, even if you have authorized access, is prohibited.
  - Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal.

Unacceptable Uses of EHI

- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- Providing information about or lists of ASC employees to parties outside the ASC.

Unacceptable Uses of EHI

- Example of some policy guidelines to have in place that outline the following activities as strictly prohibited, with no exceptions for **Email and Communication Activities:**
  - Sending **unsolicited** email messages, including the sending of "junk mail" or other advertising material to individuals who did **not specifically request such materia**l (email spam).
  - Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies
  - Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

Unacceptable Uses of EHI

- Blogging & Social Media by employees, whether using facility's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of facility's systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate facility's policy, is not detrimental to facility's best interests, and does not interfere with an employee's regular work duties. Blogging from the facilities systems is also subject to monitoring.

Unacceptable Uses of EHI

- The facility's Confidential Information policy also applies to blogging and social media. As such, employees are prohibited from revealing any facility confidential or proprietary information, trade secrets or any other material covered by facility's Confidential Information policy when engaged in blogging.

Unacceptable Uses of EHI

- Employees may also not attribute personal statements, opinions or beliefs to facility when engaged in social media. If an employee is expressing his or her beliefs and/or opinions in social media, the employee may not, expressly or implicitly, represent themselves as an employee or representative of ASC's Name.

Unacceptable Uses of EHI: Patient Emails

- **Can we use e-mail to discuss health issues and treatment with our patients?**
  - Yes. The Privacy Rule allows covered health care providers to communicate electronically, such as through e-mail, with their patients, provided they apply reasonable safeguards when doing so.

Unacceptable Uses of EHI: Patient Emails

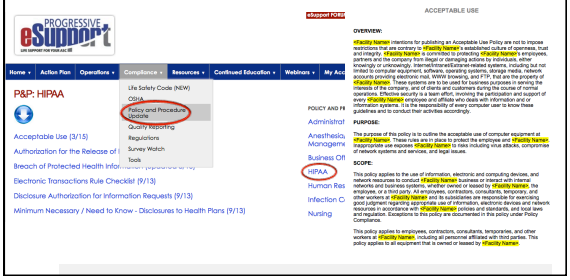
- Take certain precautions:
  - Avoid unintentional disclosures, such as checking the e-mail address for accuracy before sending, or sending *an e-mail alert to the patient for address confirmation prior to sending the message, such as a patient portal.*
  - Limit the amount or type of information disclosed through unencrypted e-mail.
  - In addition, covered entities will want to ensure that any transmission of electronic protected health information is in compliance with the HIPAA Security Rule requirements at 45 C.F.R. Part 164, Subpart C.

Unacceptable Uses of EHI: Patient Emails

- If the use of unencrypted e-mail is unacceptable to a patient who requests confidential communications, other means of communicating with the patient, such as by more secure electronic methods, or by mail or telephone, should be offered and accommodated.
- Patients may initiate communications with a provider using e-mail. If this situation occurs, the health care provider can assume (unless the patient has explicitly stated otherwise) that e-mail communications are acceptable to the individual.
- If the provider feels the patient may not be aware of the possible risks of using unencrypted e-mail, or has concerns about potential liability, the provider can alert the patient of those risks, and let the patient decide whether to continue e-mail communications.

Available on eSupport

Compliance/Policy & Procedure Update/Acceptable Use



Breach

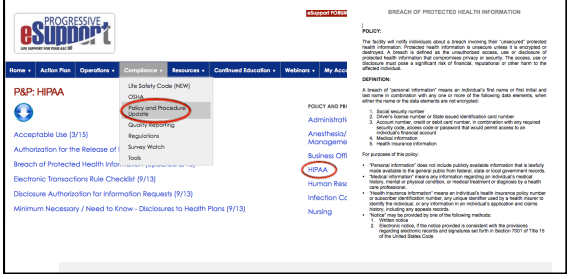
- **Definition of a breach of "personal information" means** an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:
  1. Social security number.
  2. Driver's license number or State issued Identification Card number.
  3. Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.
  4. Medical information.
  5. Health insurance information.

Breach: Examples

- $4.8M New York and Presbyterian Hospital (NYP) – internet access to server
- $800K Parkview Health System, Inc. - MD patient records delivery
- $150K Adult & Pediatric Dermatology, P.C., of Concord, Mass - lost thumb drive

Available on eSupport

Compliance/Policy & Procedure Update/Breach of Protected Health Information



HIPAA and Cash Paying Clients

- **A Patient's Right to Restrict Disclosure of Protected Health Information when Paying Out of Pocket** HIPAA 45 CFR 164.522(a)(vi)) 78 Fed. Register 5566, 5626-5630.
- If a patient has paid in full for a service or item, out of pocket, then the patient may require that the health care provider not disclose PHI pertaining to the service or item to a health plan when carrying out payment or other health care operations functions.

HIPAA and Cash Paying Clients

- **Medicare rules require "participating" physicians to submit claims for Medicare patients. Generally, such provider may not collect the full charge in advance, from Medicare patients. Does the new regulation create an exception to this rule?**
- Yes. The new HIPAA rule regarding cash payment effectively trumps the general Medicare rule that the participating physician may not collect payment in full from Medicare patients. In the 2013 guidance, HHS notes an existing proviso in Medicare law that if a Medicare patient refuses, of his/her own free will, to authorize the submission of a bill to Medicare, then the ASC is *not* required to submit a claim to Medicare for the covered service and may accept an out-of-pocket payment, in full, from the patient.

HIPAA and Cash Paying Clients

- **What other obligations are triggered by the cash-payment rule discussed above?**
- The provider must revise its Notice of Privacy Policies as necessary to include a specific statement that patients have a right to restrict certain disclosures of PHI to a health plan where the patient pays out of pocket, in full, for the health care item or service. The ASC should also identify workforce members whose job functions will be affected by the new regulation, and train those workforce members in implementing these expanded patient rights. The ASC should also evaluate its electronic systems to determine if information subject to a required restriction can be flagged or segregated in the system to ensure the information is not disclosed to health plans. Some ASC may need to invest in upgraded systems in order to meet these requirements.

HIPAA and Cash Paying Clients

- **What penalties are applicable if the provider fails to comply with the cash-payment provision?**
- The ASC will be subject to civil monetary penalties up to $50,000 per violation. Depending on the exposure, the penalty must be a minimum of $1,000 per violation. If the violation is due to willful neglect, but is promptly corrected (within 30 days), the penalty must be a minimum of $10,000 per violation If the violation is due to willful neglect, and is not corrected within 30 days of the date that the provider knew, or should have known of the violation, the penalty is $50,000 per violation.

HIPAA and Cash Paying Clients

- **When is an ASC permitted or required to disclose the restricted PHI, despite the patient's request?**
- ASCs remain obligated to make disclosures of PHI as *required by law*. "Required by law" is defined as a mandate contained in law (including state or other law) that compels an ASC to make a use or disclosure of PHI and that is enforceable in a court of law. For purposes of this definition, "required by law" includes:
  - Medicare conditions of participation with respect to health care ASCs participating in the program;
  - Court orders and other legally mandated disclosures; and
  - Statutes and regulations that require the production of information if payment is sought under a government program providing public benefits.

HIPAA Tool Kit

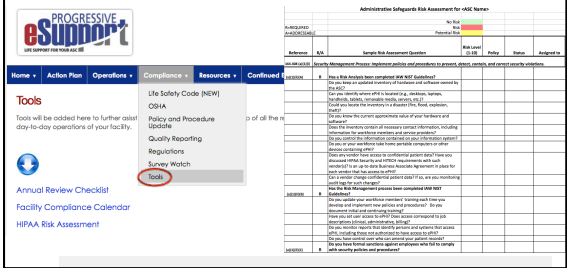
- A summary documentation of all electronic sources and media that fall under HIPAA.
- An administrative risk assessment tool for the Security Management Process: Implement policies and procedures to prevent, detect, contain, and correct security violations.
- A physical risk assessment tool for Facility Access Controls: Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

HIPAA Tool Kit

- Technical Risk Assessment tool to monitor Access Controls: Implement technical policies and procedures for electronic information systems that maintain EPHI to allow access only to those persons or software programs that have been granted access rights as specified in Sec. 164.308(a)(4).
- A breach assessment tool to summarize the facilities exposure to a potential breach.

Available on eSupport

Compliance/Tools/HIPAA Risk Assessment



Administrative Safeguards Risk Assessment for <ASC Name>

Reference	N/A	Sample Risk Assessment Question	Risk Level (1-10)	Policy	Status	Assigned to
164.308 (a)(1)(i)		*Security Management Process: Implement policies and procedures to prevent, detect, contain, and correct security violations.*				
164.308(a)(1)(ii)	R	**Has a Risk Analysis been completed IAW NIST Guidelines?**				
		Do you keep an updated inventory of hardware and software owned by your ASC?				
		Can you identify where ePHI is located (e.g., desktops, laptops, handhelds, tablets, removable media, servers, etc.)?				
		Could you locate the inventory in a disaster (fire, flood, explosion, theft)?				
		Do you know the current approximate value of your hardware and software?				
		Does the inventory contain all necessary contact information, including information for workforce members and service providers?				
		Do you control the information contained on your information system?				
		Do you control access to the home portable computers or other devices containing ePHI?				
		Can a vendor change confidential patient data? If so, are you monitoring audit logs for such changes?				
		Has the Risk Management process been completed IAW NIST Guidelines?				
164.308(a)(5)(i)	R	**Do you update your workforce members' training each time you develop and implement new policies and procedures? Do you document initial and continuing training?**				
		Have you set user access to ePHI have access correspond to job responsibilities and to the minimum ePHI needed?				
		Do you monitor reports that identify users and systems that access ePHI, including those not authorized to have access to ePHI?				
		Do you have control over who can amend your patient records?				
164.308(a)(1)(iii)	R	**Do you have formal sanctions against employees who fail to comply with security policies and procedures?**				

Closure

- Basic security measures can be highly effective and affordable. Using your risk assessment tool kit, discuss and develop an action plan to mitigate the identified risks. The plan should have five components: administrative, physical, and technical safeguards; policies and procedures; and organizational standards.

Closure: Risk Management

- Manage and mitigate risks. Begin implementing your action plan. Develop written and up-to-date policies and procedures about how your ASC protects e-PHI. Retain outdated policies and procedures.
- Prevent common mistakes by holding workforce training. To safeguard patient health information, your workforce must know how to implement your policies, procedures, and security audits. HIPAA requires you as a covered provider to train your workforce on policies and procedures. Also, your staff must receive formal training on breach notification.
- Communicate with patients. Your patients may be concerned about confidentiality and security of health information in an EHR. Emphasize the benefits of EHRs to them as patients, perhaps using patient education materials available in the Privacy & Security Resources section.

Still not on Progressive eSupport?

- Request your free web demo today!
  - Visit www.progressivesurgicalsolutions.com/esupport
  - Email us at info@pss4asc.com
  - Or call us! (855) 777-4272

Questions??

Email your questions regarding today's content to:

info@pss4asc.com

Mark your calendars!

Join us next time for:

Quality Net Reporting

May 18, 2015
11AM PT/2PM ET

Sarah Martin, MBA, RN, CASC
Progressive Surgical Solutions

Brought to you by 

Introducing…

A NEW webinar series
PROGRESSIVE HALF TIME

Friday, April 24, 2015
11AM PT/2PM ET

LIFE SAFETY CODE
Bill Lindeman, AIA

$75
FREE for eSupport members!!

Brought to you by