Updated Basic HIPAA/HITECH Awareness Training **for Health Care Staff**

First Name

Last Name

E-mail

Organization Name

Final HIPAA Rule

• On September 23rd 2013, all Covered Entities (CE) and Business Associates (BA) must comply with the HITECH Final Rule that modifies HIPAA.

• It raises the requirements for patient privacy, and increases the penalties for non-compliance.

• All CEs and BAs should take these changes very seriously and ensure staff members understand their responsibilities before the new rule takes effect.

 web: ehr20.com E-mail: info@ehr20.com Call: 802-448-2255

Who Needs this Training?

- This training is intended for any CEs and BAs handling Protected Health Information of patients under HIPAA rule.
- All physicians, contractors, volunteers, or others that use or have access to patient information should also be aware of the changes.

What has Changed?

The three areas of the Final Rule that all staff members should know are:

1. Privacy

Some privacy issues that you could address internally under the old rules will now have to be reported to the Department of Health and Human Services (DHHS).

2.Penalties

If DHHS determines the covered entity or business associate was negligent they could face significant financial penalties.

3. BAs

HIPAA Rules now directly apply to all Business Associates, but Covered Entities can be held responsible for their actions.

 web: ehr20.com E-mail: info@ehr20.com Call: 802-448-2255

Final Rule

According to the Final Rule, most unauthorized uses or disclosures of Protected Health Information (PHI) will likely be considered breaches. It is now more important than ever that each staff member remembers:

- what is expected of them each day to protect patient information and minimize unauthorized uses and disclosures of PHI
- how to report their concerns if they suspect PHI has been disclosed, exposed, or misused in ANY way

Protect

Each of you has a responsibility to PROTECT PHI.

- Continue to make the protection of patient information the highest of priorities.
- Do not share PHI with anyone who is not authorized to have it.
- Do not access PHI unless you have a work-related reason to view it or an authorization form on file signed by the patient granting you permission.
- Only access the minimum amount of information necessary to do your job or fill an authorized request.
- If you are not sure call your organization's Privacy Office before you access or provide PHI to someone else!

 web: ehr20.com E-mail: info@ehr20.com Call: 802-448-2255

Report

If you believe or suspect that PHI may have been put at risk you have a responsibility to REPORT those concerns to your organization's Privacy or Compliance Office immediately.

- The new rule shortens the time frame in which you must investigate and report any findings.
- The minute you believe there is a problem, you need to notify the appropriate authorities.
- The sooner you notify the better chance your organization has to limit the damage to the individuals involved.

Mobile Devices and Storage Media

Staff members who use mobile devices or storage media take on additional responsibilities to protect the information they place on these devices.

Mobile Devices

Laptops
Smart Phones
Tablets
Cameras

Storage Media

CDs/DVDs
USB Drives
Memory Cards
Portable Disks, etc.

- Do not store PHI on Mobile Devices or External Storage Media unless it is absolutely necessary.
- If it is necessary then the device MUST be encrypted and password protected where technically feasible.
- If not technically feasible, then other alternate safeguards such as increased physical security must be applied.

Lost or Stolen Devices

- If any Mobile Device or Storage Media is lost or stolen you must report it to your organization's Help Desk, Privacy Office, or Compliance Office immediately.
- If you use your personal cell phone for work-related reasons it must also be encrypted and if it is lost or stolen you must report it, as well.

Why Protect and Report?

- Covered Entities and Business Associates are required by law to report breaches to HHS
- When a breach is reported, essentially a violation of the Privacy Rule(HIPAA) is reported
- If HHS suspects that the breach or violation resulted from "willful neglect," they will conduct a compliance review
- Covered Entities and Business Associates can be fined as much as $50,000 per violation of each provision of HIPAA

Breach Response

Two things can increase the amount of the fines:

- **Willful neglect**
  - This means acting in a manner that shows conscious, intentional failure or reckless indifference towards our obligation to comply with the HIPAA rules
- **Failure to correct the violation quickly**
  - Do not delay reporting to your Privacy Officer any incident that you know or think might be a HIPAA violation!

Unauthorized Uses and Disclosures

Here are some types of unauthorized uses and disclosures to be particularly alert to avoiding:

- Fax sent to the wrong number
- Patient statements or discharge papers given to the wrong patient
- Envelopes not sealed
- Un-encrypted mobile devices or storage media
- Unauthorized patient pictures or information posted on social media web sites
- Accessing patient information that is not job-related
- Disposing of patient information incorrectly

Your Responsibilities

You must act honestly, diligently, and quickly to prevent and address incidents related to PHI. Therefore, your responsibilities are:

- to be diligent in your protection of PHI
- if you ever feel PHI has been compromised in any way, contact your organization's Privacy or Compliance Office and report it immediately.

Business Associates

- Another area that the Final Rule has strengthened is how Business Associates must comply with HIPAA Laws
- Almost any vendor who has access to PHI is a business associate, and you can be held responsible if they are not compliant with these laws

Business Associates

If you work with any vendor who has access to PHI you must verify they have completed the appropriate paperwork with your organization's legal department:

- If you are unsure, ask and verify.
- Do not sign any documents that a vendor asks you to sign without first reviewing those documents with the legal department.

Assessment Question 1

Under what conditions can I save PHI to a USB flash drive?

- ☐ A. If the flash drive is encrypted.
- ☐ B. If the file is encrypted with an approved encryption product.
- ☐ A or B
- ☐ None of the above

Correct Answer: B
Only when mobile devices are encrypted with an approved encryption product PHI information should be stored.

Assessment Question 2

What is your responsibility to the New Rule?

- ☐ A. Nothing is different
- ☐ B. Protect PHI
- ☐ C. Do not disclose PHI unless an authorization is on file
- ☐ D. Report any inappropriate use or disclosure of PHI
- ☐ B & D

Correct Answer: B & D
Final rule has introduced several new requirements. However, protecting PHI and reporting is one of the key requirements.

Assessment Question 3

What is significant about the change to the definition of a breach under the final rule?

- ☐ Breach is presumed following every impermissible use of PHI
- ☐ Harm standard was reinforced to include additional categories
- ☐ Penalties were waived for less than 250 records disclosed
- ☐ Exceptions to notifications requirements were eliminated

Correct Answer #1 - Breach is presumed following every impermissible use or disclosure of PHI. The CE must demonstrate through a properly conducted and documented risk assessment that there is a low probability of compromise of the affected data/PHI.

Assessment Question 4

Which of the following steps is not necessarily part of a security incident response?

- ☐ Conducting risk assessment
- ☐ Drafting a business risk assessment plan
- ☐ Notification to affected individuals
- ☐ Mitigation efforts

Correct Answer #2. Ideally a risk assessment plan or process is already in place prior to discovery of a security incident, based upon existing HIPAA requirements, and good business practice, which will be addressed later in the presentation. The other items would typically be initiated after incident discovery, though not necessarily in the order listed.