ONE DAY IN-DEPTH TRAINING

HIPAA - Ransomware - Privacy - Security - Breach - MIPS Security Risk Assessment

Covered Entities and Business Associates Should Attend

HIPAA

--- compliance simplified ---

2017

Save the Date: October 26, 2017

Brought to you by

HITECH Associates Compliance HipaaComplianceKit.com

The Leader in HIPAA Compliance Products and Services.

Stay fully compliant with Office for Civil Rights Guidelines and Regulations

Does a Representative From Your Office Need to Attend?

If you answer No to any of the following questions, sign up today.

Does your office have a flat fee of $6.50 for medical records provided to patients?	Yes	No
Is your Notice of Privacy Practices posted in your lobby and on your web site's home page?	Yes	No
Do you have fully executed Business Associate Agreements with all your business associates?	Yes	No
Has your practice completed a comprehensive risk assessment in the past 12 months?	Yes	No
Do you have a documented Risk Management Plan that shows progress on your Action Items?	Yes	No
Have you reported a breach to the Office for Civil Rights in the past year?	Yes	No

Review of the 2017 HIPAA Audits by the Office for Civil Rights

The above questions and more were a part of the Office for Civil Rights recent audits of small medical practices. As many as 94% of the offices audited failed on these basic HIPAA requirements. HIPAA has changed and if you have not kept up with the changes you open yourself to massive fines and loss of reputation. OCR published Access Guidance concerning your requirements to provide patients with copies of their medical records. Changes you must implement are a flat fee or cost based fee for medical records, digital delivery of medical records, release of all the records your practice maintains on the patient and a requirement to email patients medical records after a "light warning". The Notice of Privacy Practices was a focal point of the audits. Notice of Privacy Practices must be updated for Omnibus, list any interfaces you have with your EHR, be posted prominently on your web site, be downloadable, be posted in your lobby and the Notice notification signed by patients must be updated every 3 years.

The HIPAA Compliance Officer Full Day Seminar will review and explain all of the above and the other changes to HIPAA as well as an in-depth review of the basics. The HIPAA Security Rule requires the protections your organization must have in place to protect and recover from Ransomware. Ransomware is an epidemic in health care and it is a problem that is getting worse every day. New strains of Ransomware now copy and exfiltrate your files to their cloud based server. If you do not pay the ransom, they will release your patient information onto the Internet. At this seminar we will update you as to best practices to avoid and recover from ransomware based on industry reports, OCR, NIST documentation, FBI guidance and actual experience with our clients and how they responded to malware incidents.

Seminar Topics Will Include

- Permitted Disclosures
- Authorization Forms – Required Elements
- Subpoenas – When Authorization is Required
- Patient Testimonial – HIPAA Requires
- Responding to Negative Online Patient Reviews
- Talking with Family & Friends – New OCR Guidance
- Who Are Your Business Associates
- When You Need A Business Associate Agreement
- Alternatives to Signing a BAA
- Ransomware and It's Impacts
- Ransomware is a HIPAA Breach – When to Report
- Reasonable & Appropriate Security
- Allowable Fees for Patient Records
- Access Requirements
- Equipment Disposal – Must Have HIPAA Certification
- MIPS Security Risk Assessment
- Developing A Culture of Compliance
- HIPAA Audits and Investigations
- Required Documentation is Key
- HIPAA Compliant Email & Texting
- Audit Log Reviews

Seating is limited - Reserve your seat today!

Course Content

Complete with Video Clips From This Year's Security Conference.

HIPAA Compliance Officer Basics

This course will provide an overview of your HIPAA requirements and provide insight on what your organization must do to be HIPAA compliant. A full review of HIPAA documentation requirements, breach review and other topics will be covered.

Reasonable Security – Not Perfect Security

The HIPAA Security Rule is a one size fits all. We will help you determine what is reasonable security for your office. Reasonable security is your key to avoiding HIPAA fines when something does go wrong, such as a Ransomware attack, and the odds are it will happen to you.

Ransomware and Other Malware – Security Incident Planning

Putting in the protections to deter and avoid a security incident are just the beginning, you must be able to quickly recover and perform forensic reviews to avoid a reportable breach. The burden of proof is on your organization, if you cannot prove a full breach did not occur, the default position is that a breach did occur.

Securing Mobile Devices and Remote Access

Mobile devices are major security risks to your organization. We will show you how to use and secure these devices to be HIPAA compliant. Remote access has been a common method of intrusion by cybercriminals, learn how to protect your network.

Business Associates and Your Risk

Business Associate Agreements have been a major focus of the Office for Civil Rights. Fines for not having these agreements ranged from $750,000 to $5.5 million last year. We will review who is a business associate, who is not a business associate and when you can treat a vendor as a "workforce member".

HIPAA Required Auditing of Access to PHI

Being proactive to security events is required and auditing of access to patient information is required. Your office should be documenting system activity reviews on a monthly basis. We call it your HIPAA homework. The Office for Civil Rights put out additional guidance on what they expect to be audited and we will be reviewing those requirements.

Upcoming Requirements – The Task Force Report

The Office for Civil Rights commissioned a Task Force to discuss and develop recommendations for the growing challenge of cyber attracts targeting health care. As this report has been sent to congress there is a good chance we will see these recommendations enacted into the HIPAA Security Rule. We will review the 6 Major Imperatives, Recommendations and Action Items form the report.

MIPS Overview and the Security Risk Assessment Requirement

MIPS has replaced "meaningful use" and the requirement for a Security Risk Assessment is included. Our MIPS expert will give a quick review of MIPS and offer insight into meeting the new payment methods.

Course Content is Subject to Change

Seminar attendees will receive a course book to review the day's training and digital files of all slide presentations along with a complete reference guide and HIPAA documentation. Video of the seminar will also be provided.

Protecting Patient Privacy .com

HITECH Associates
Compliance HipaaComplianceKit.com
3905 Tampa Road, Suite 213
Oldsmar, Florida 34677
813-892-4411

The HIPAA Seminar
October 26th

What your collegues have said about our previous seminars.

Very well conducted. Helpful, informative people, class was very informational. Will recommend to others.

Best inservice we've ever had. Focused on what was important.

Your a huge help!

☐	**YES!** I am ready to get fully HIPAA compliant and protect the privacy of our patients for only $249. Lunch and snacks are provided.
Seminar Location & Time	Hilton Tampa Airport Westshore 2225 North Lois Avenue Tampa, Florida 33607 Hotel Phone #: (813) 874 5019 October 26, 2017 9:00 am to 4:00 pm
Name of Organization	
Address	
City State Zip	
Phone	
email	
Attendee 1	
Attendee 2	
Attendee 3	
Discount	If more than one person from an organization attends the conference the rate per attendee drops to $200 per attendee. *HITECH clients, call for your special pricing.*
Payment & Registration	Fax this form to 877-667-5177 or email to mm@HipaaComplianceKit.com and we will send you a customized invoice. Tuition is due before the seminar.