

Webinar on

Breach Response Training

• Learning Objectives

- ☐ *Breach Laws*
- ☐ *Breach Identification*
- ☐ *Breach Risk Assessment*
- ☐ *Policies and Procedures*
- ☐ *Breach Response Plan*
- ☐ *Getting through a Breach Investigation*

In this webinar you will learn - what need to know to identify and report a breach and how you can report breaches to the OCR portal without fear of investigation.

PRESENTED BY:

Michael McCoy - has been performing HIPAA risk assessments for the past 8 years. With over 1000 clients, Michael has a wide breadth of experience in dealing with all HIPAA matters and the Office for Civil Rights. Michael's background before going into HIPAA was 23 years in the medical field performing Administration and Marketing.

On-Demand Webinar

Duration : 60 Minutes

Price: \$200

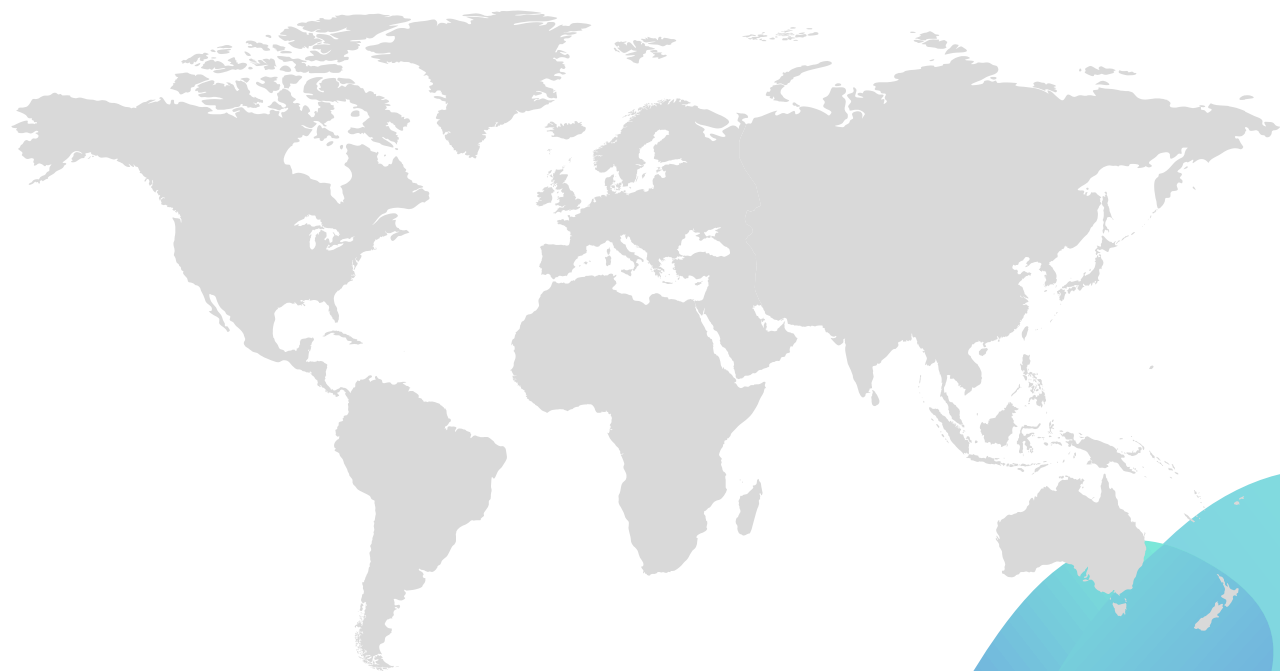
Webinar Description

The topic is breaches of the impermissible use or disclosure of protected health information and for state law, personal information. A breach risk assessment is required with 4 questions that must be addressed. We will review the breach risk assessment, identifying a breach, no breach is too small to review and report, and what to do when a major breach (500 records) or more is involved. With a major breach, you must follow your breach plan. That means you need to have a breach plan in place. (We will provide one for all attendees) Expect a full investigation from the OCR to include your risk assessment, policies and procedures, and other required HIPAA documentation. Past investigations we have been involved with required between 400 – 600 pages of documentation to be submitted. In addition, you may have state reporting requirements. All patients must receive letters informing them of the breach, the media must be alerted and other specific requirements must be performed or your office could face massive fines. Even if your business associate caused the breach, you are not off the hook. We'll review how to address this threat and reduce your exposure.



Who Should Attend

Practice Managers, C-suite executives, HIPAA Compliance Officers. This webinar is for covered entities (hospitals, physicians, labs, etc.) and (business associates) businesses that work with them like shredding companies, billing companies, consultants.



Why Should You Attend ?

Miss a breach deadline, get fined \$250,000. Don't report a breach and face millions of dollars in fines. For HIPAA a suspected breach is an actual breach and you must have the documentation showing that no breach occurred. You are guilty until proven innocent. Federal and state breach rules require that your staff be able to identify a breach and your office must properly respond. No breach Response Plan in place, face more millions of dollars in fines. And it is not just your organization, you are responsible, legally and financially, for your business associates. The Office for Civil Rights tells us they check the breach portal when investigating your office for any reason. No reported breaches (required to be reported at the end of the year) well that is a red flag, what other HIPAA documentation are you missing? We will show you how to avoid breaches, how to report breaches using the required Breach Risk Assessment, and teach your staff what they need to know to identify and report a breach and how you can report breaches to the OCR portal without fear of investigation.



To register please visit:

www.grceducators.com
support@grceducators.com
740 870 0321