GRC Online Training Hub
EDUCATORS
Axons Technology and Solutions

Webinar on

E-Mailing, Texting, and the Use of Personal Devices by Health Care Professionals – HIPAA and Privacy Myths vs Reality

Learning Objectives

- *The basics of HIPAA privacy*
- *The basics of HIPAA and the use of electronic communications*
- *Examples of state licensure laws governing protected health information*
- *Elements of privacy notices and communications practices with patients*
- *Bonus: website confidentiality and privacy disclaimers for the health care practitioner with their own website*

GRC Online Training Hub
EDUCATORS
Axons Technology and Solutions

This webinar is thus an advanced overview of the many rules, both by HIPAA at the federal level and in state licensure laws, that govern e-mailing and texting with the patient and with other health care practitioners.

PRESENTED BY:

Mark R. Brengelman focuses on representing health care practitioners before licensure boards and in other professional regulatory matters. He also represents children as Guardian ad Litem and parents as Court Appointed Counsel in confidential child dependency, neglect, and abuse proceedings in family court.

GRC Online Training Hub EDUCATORS
Axons Technology and Solutions

On-Demand Webinar

Duration : 60 Minutes

Price: $200

Webinar Description

This informative webinar begins with the most basic of questions: Does the HIPAA Privacy Rule permit health care providers to use e-mail to discuss health issues and treatment with their patients?

Find out the answer and examine how the privacy rules of HIPAA allow covered entities and health care providers to communicate electronically, such as through e-mail or texting, with their patients and with other health care practitioners, but only provided those health care practitioners apply reasonable safeguards when doing so. This is mandated by federal administrative regulation. Specifically, certain precautions need to be taken when using e-mail to 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.

Further, while the HIPAA privacy rules do not prohibit the use of unencrypted e-mail for treatment-related communications between health care providers and patients, other safeguards should be applied reasonably to protect privacy, such as limiting the amount or type of information disclosed through the unencrypted e-mail. The health care practitioner may include the least amount of protected health information in an unencrypted e-mail. In addition, covered entities must make sure any transmission electronically of protected health information follows the HIPAA Security Rule requirements of federal law.

Patients have the right under the HIPAA privacy rules to request and have a covered health care provider communicate with them by alternative means or at alternative locations, if reasonable. For example, a health care provider should accommodate an individual's request to receive appointment reminders via e-mail, rather than on a postcard, if e-mail is a reasonable, alternative means for that health care practitioner or provider to communicate with the patient.

However, 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. The patient may also designate a particular e-mail address to use, such as the patient's personal e-mail and not their work e-mail.

Patients may even initiate communications with a health care practitioner or other 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. This is implied consent and implied usage. If the health care practitioner or other 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.

Uncertainty exists when faced with strict laws. Erase the fear, uncertainty, and doubt by reviewing how patient consent and communication practices can be updated to allow for specific means of electronic communication. Further erase the uncertainty, fear, and doubt about what other laws, such as state licensure laws, apply to the confidentiality of patient protected health information. Review further some examples of specific state licensures laws that apply to electronic communications that may be stricter than even HIPAA itself.

This webinar is thus an advanced overview of the many rules, both by HIPAA at the federal level and in state licensure laws, that govern e-mailing and texting with the patient and with other health care practitioners.

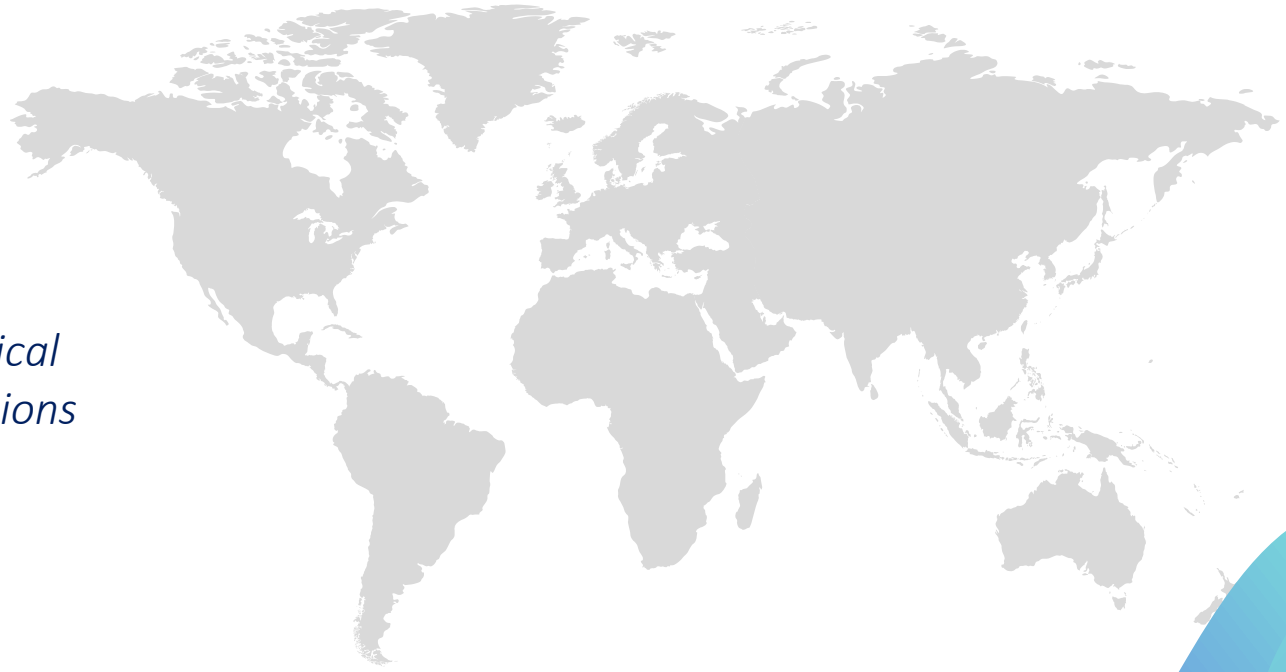
Who Should Attend ?

Individual health care practitioners

Health care attorneys

Teachers and educators in graduate-level medical education across the many health care professions

Corporate counsel in health care

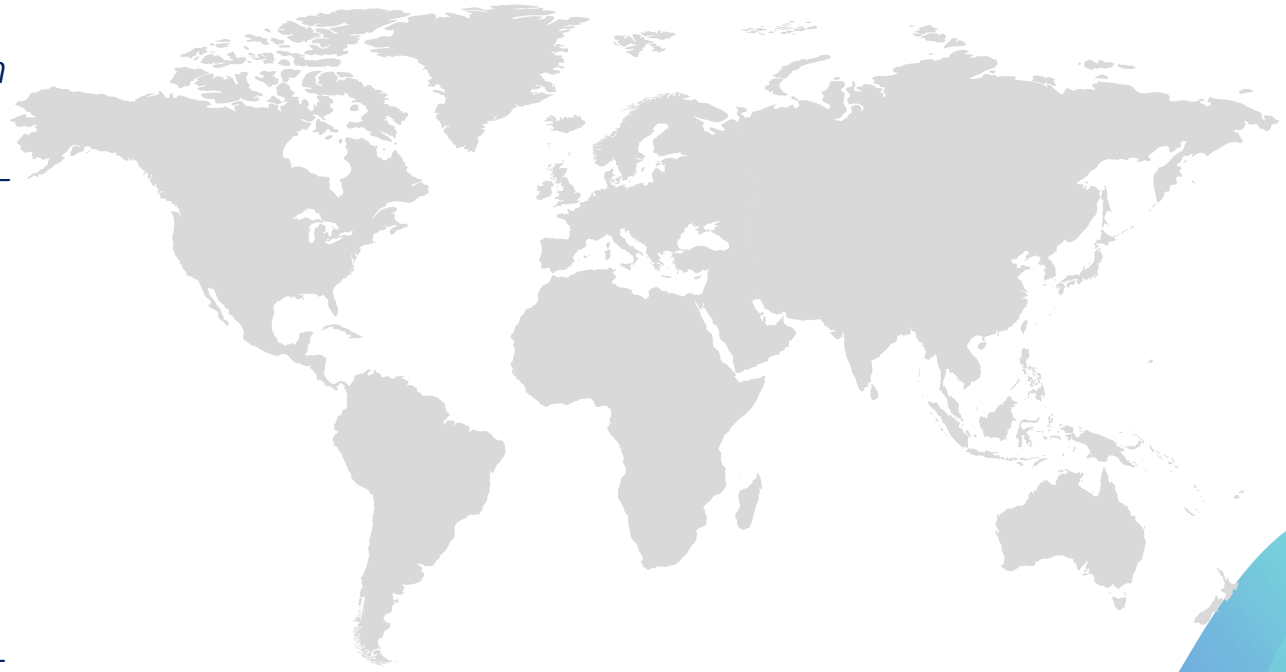


GRC Online Training Hub
EDUCATORS
Axons Technology and Solutions

Why Should Attend ?

While the basic provisions of privacy for protected health information are well known, their application in today's world of electronic and personal communication devices is complex – such as texting, e-mailing, and using personal devices such as smart phones and tablet computers. In addition to HIPAA rules, various state licensure laws exist to require confidential information to be kept confidential.

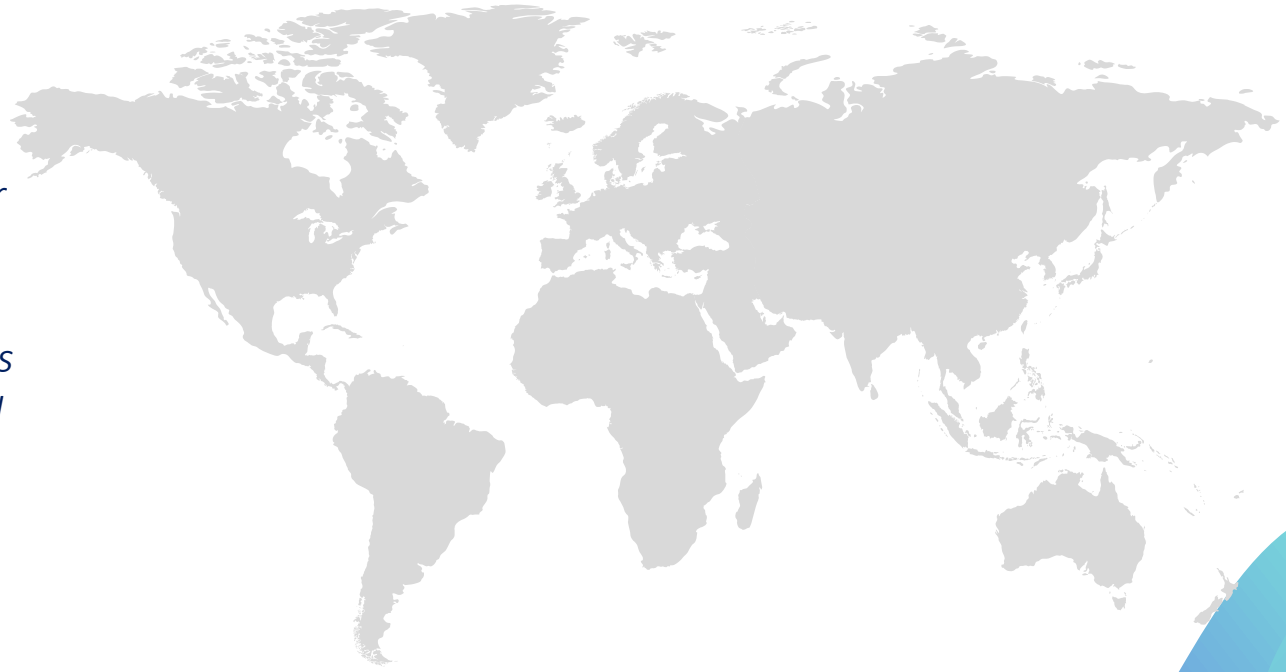
Many security rules regarding protected health information involving how and when protected health information is to be kept confidential and not accessible to others outside of direct patient care. But what is protected health information? Can communications not involve such protected health information be transmitted by non-confidential and non-secure methods? Is even a patient name protected health information?



GRC Online Training Hub EDUCATORS
Axons Technology and Solutions

The ability to text or e-mail health care practitioners and other staff and patients has become a priority for many health care entities and practitioners, especially solo health care practitioners with limited support staff. Maintaining patient privacy and confidentiality is necessary to make sure covered entities meet compliance standards of HIPAA and state licensure laws. Although e-mailing and texting are convenient for the health care practitioner and patient, these communication methods have security risks and inherent pitfalls. Implementing e-mail and text solutions in the health care setting is a complex issue and several factors must be addressed.

Erase the fear, uncertainty, and doubt about exactly how a health care practitioner may use modern texting and e-mail, both within their own health care organization or facility and to the outside world of patients. Find out how these communications may or may not be required to be retained by the health care practitioner. Finally, examine easy guidelines for the health care practitioner in a solo or small group setting can use e-mail and texts without violating patient confidentiality under HIPAA as well as state licensure laws.



GRC Online Training Hub
EDUCATORS
Axons Technology and Solutions

GRC Online Training Hub
EDUCATORS
Axons Technology and Solutions

To register please visit:

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