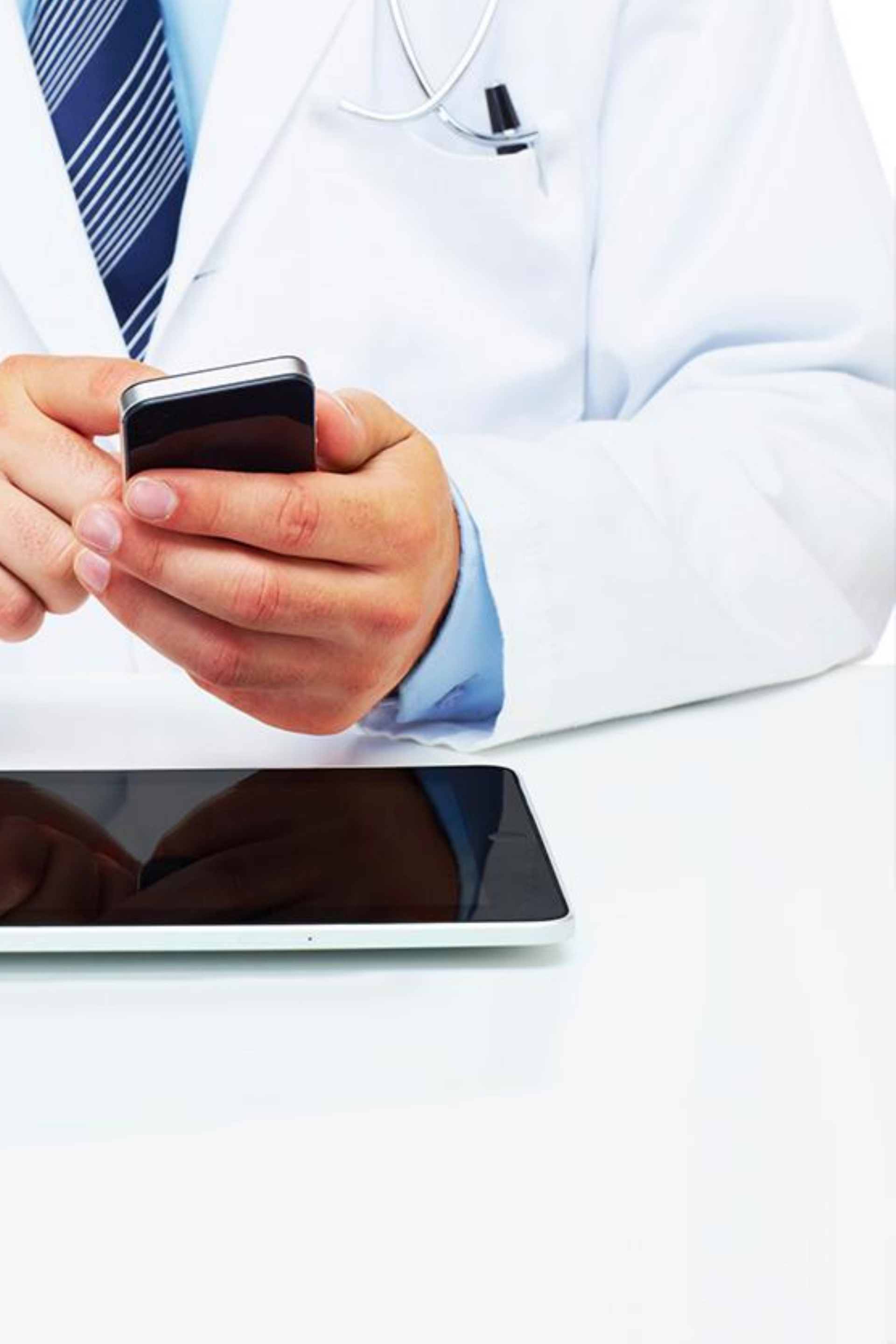


Text or Not to Text
No Longer the Question

Managing Risk of Medical Texting

James Ronald Kennedy, MHA, MJ, ARM
LAMMICO Risk Management Consultant

LAMMICO

Legal Requirements: Federal & State

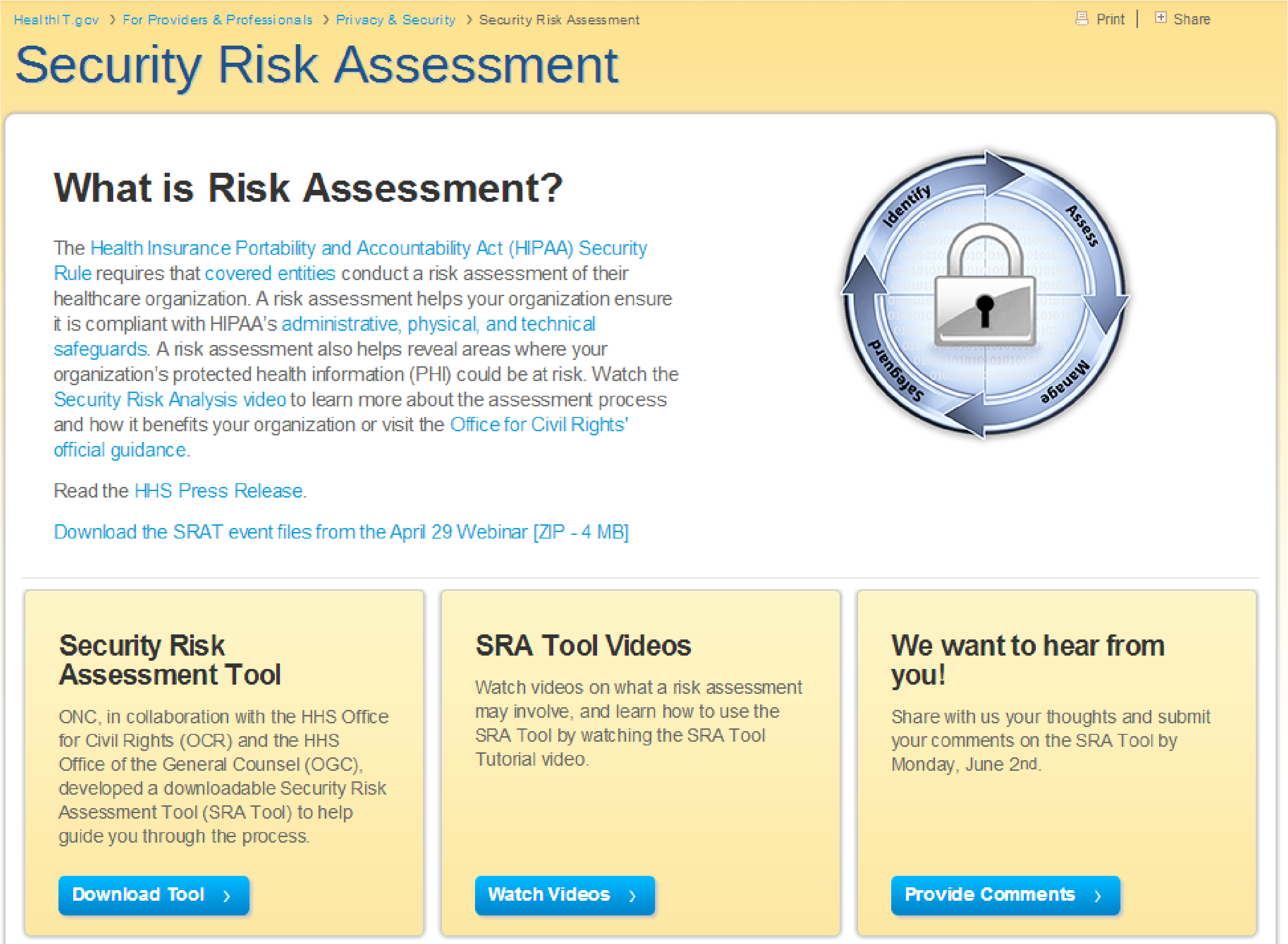
- Federal via HIPAA
  - Privacy
  - Security
  - Retention
  - Patient Access
- State
  - Preservation of medical records
  - Data breach obligations
  - Production of medical records
    - Civil or criminal investigation/litigation

Before Texting: Risk Assessment

- HIPAA requirement for all medical records
  - Includes e-PHI (electronic protected health information)
  - HIPAA compliant risk assessment
    - "Conduct an accurate and through assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (e-PHI) held by the organization"
    - HIPAA's security rule establishes risk assessment as one of the four required implementations

http://www.healthit.gov/providers-professionals/security-risk-assessment

Before Texting: Risk Assessment



HealthIT.gov › For Providers & Professionals › Privacy & Security › Security Risk Assessment
Print | Share
Identify
Assess
Manage
Safeguard

Security Risk Assessment

What is Risk Assessment?

The Health Insurance Portability and Accountability Act (HIPAA) Security Rule requires that covered entities conduct a risk assessment of their healthcare organization. A risk assessment helps your organization ensure it is compliant with HIPAA's administrative, physical, and technical safeguards. A risk assessment also helps reveal areas where your organization's protected health information (PHI) could be at risk. Watch the Security Risk Analysis video to learn more about the assessment process and how it benefits your organization or visit the Office for Civil Rights' official guidance.

Read the HHS Press Release.

Download the SRAT event files from the April 29 Webinar [ZIP - 4 MB]

Security Risk Assessment Tool

ONC, in collaboration with the HHS Office for Civil Rights (OCR) and the HHS Office of the General Counsel (OGC), developed a downloadable Security Risk Assessment Tool (SRA Tool) to help guide you through the process.

SRA Tool Videos

Watch videos on what a risk assessment may involve, and learn how to use the SRA Tool by watching the SRA Tool Tutorial video.

We want to hear from you!

Share with us your thoughts and submit your comments on the SRA Tool by Monday, June 2nd.

Before Texting: Risk Assessment

- HIPAA requirement for all medical records
  - Three questions to determine if you are in compliance
    1. Have you identified the e-PHI within your organization?
       - This includes e-PHI that you create, receive, maintain or transmit
    2. What are the external sources of e-PHI?
       - For example do vendors, consultants or patients create, receive, maintain or transmit e-PHI?
    3. What are the human, natural, and environmental threats to information systems that contain e-PHI?
- HIPAA rules indicate that risk assessment is a necessary tool for reaching compliance

Before Texting: Risk Assessment

- Periodic review and updating of risk assessment
  - “The risk analysis process should be ongoing”
  - “The Security Rule does not specify how frequently to perform risk analysis”
  - “Some covered entities (CEs) may perform these processes annually or as needed (e.g., bi-annually or every 3 months) depending on circumstances of their environment”
  - “Risk analysis is the first step in an organization’s Security Rule compliance efforts”

How Much Texting Are We Doing?

- Americans’ growing love of texting
  - – 2001 Americans sent 3.1 billion texts
  - – 2006 Americans sent 18.7 billion texts
  - – 2011 Americans sent 193.1 billion texts
- 72% of mobile phone users send text messages
- 73% of physicians text other physicians about work
- Organizational security policies must take into account physicians’ communication preferences

Text Must Be HIPAA Compliant **If**

- Any part of the message contains e-PHI
- Same as a letter from or to your patient regarding treatment
  - Should be included in the medical record and provide privacy, security and patient access

Text Must Be HIPAA Compliant **If**

- Any part of the message contains e-PHI
  - Created, received, transmitted or maintained by a CE
  - Including both medical and billing information

Defining e-PHI

- Electronically created, received, stored, or transmitted information "used in whole or in part, by or for the covered entity to make treatment or billing decisions about individuals"
- Examples of "identifiable" e-PHI:
  - Electronic Health Records/medical records
  - E-mail containing information regarding patient treatment/billing
  - Digitally stored video, photographs, regardless of whether or not stored in-house, by vendor, internet, cloud, flash drive, or on private devices (personal cell phones)

Does HIPAA Apply?

1. Physician text to consulting physician
   - e-PHI or not?
2. Office staff text to give patient lab results
   - e-PHI or not?
3. Patient text to a friend regarding her lab results
   - e-PHI or not?
4. Physician texting on his private phone to his wife about their neighbor’s admission to the hospital
   - e-PHI or not?

None of above precludes informal clinical conferences

Texting Inherently Risky

- "Messages containing electronic PHI can be read by anyone, forwarded to anyone, remain unencrypted on telecommunication providers' servers, and stay forever on sender's and receiver's phones"

  Andrew A. Brooks, MD, an orthopedic surgeon and cofounder and chief medical officer of Tigertext a secure mobile messaging platform

- 38% of text users have sent text message to wrong person
  - If it contains e-PHI it constitutes a reportable breach
  - Fines of $50,000 for a single violation not unusual
  - Some breaches require immediate reporting

LAMMICO

Texting Inherently Risky

- What can go wrong?
  - Theft or loss of the mobile device
  - Improper disposal of the device
  - Interception of transmission of e-PHI by an unauthorized individual
  - Lack of availability of e-PHI to persons other than the mobile device user
    - Other healthcare providers
    - Patient access as per HIPAA
    - In response to subpoena for all e-PHI

LAMMICO

Considerations When Texting e-PHI

- All forms of healthcare communications involve risk - SMS merely represent a different set of risk that must be managed
  - Risks the same - technology new and methods to manage those risks need to be specific to the new technology
  - Not that different than learning to manage new risks in your practice when a new piece of medical technology is introduced such as robotics
- Information regarding diagnosis, treatment, symptoms, appointments are (in most cases) e-PHI

LAMMICO

Considerations When Texting e-PHI

- Does your practice have a formal written policy addressing texting e-PHI?
  - Policy based on findings of documented risk assessment?
  - Addressing text messages between
    - Consulting and treating providers within practice
    - Consulting and treating providers outside of practice
    - Practice providers and office staff
    - Practice providers and patient
    - Office staff and patient

Considerations When Texting e-PHI

- Establish protocol for
  - Identifying all SMS that are authorized by the practice to text e-PHI
  - Individuals acknowledging that the practice has the right to review privately held SMS devices that are used to text healthcare data
    - This includes the right to review devices upon termination of business agreement between the practice and the individual
  - Codifying summary of text messages in the patient's medical record – not HIPAA requirement but…
  - Length of time text messages kept before deleting

Considerations When Texting e-PHI

- Establish protocol for
  - Obtaining patient’s written consent prior to initiating texting
  - Risk Management Hint: Obtain signed written consent after face to face discussion with the patient and scan signed form into patient’s medical record
    - Or place hard copy in paper record if office not using EMR
  - Patient consent contains a statement regarding the practice’s efforts to maintain privacy and security **but** that even with best efforts texting is still more risky than other methods of communication
    - Texting has a high potential for security breach

Considerations When Texting e-PHI

- Patient Consent for Texting
  - Consent should include
    - High potential for security breach statement
    - The kind of information that text messages will include
    - Who will have access to the phone on the receiving end
    - Patient agrees to delete messages within a specific time
    - Patient agrees to notify practice immediately if
      - Their phone is lost or stolen
      - They change phone number
    - Patient or practice may elect to stop texting at will
      - Notice given via text, email or in writing

Considerations When Texting e-PHI

- Patient Consent for Texting
  - Consent should include
    - Statement that only non-emergent messages should be sent
    - Statement noting that it is the patient's responsibility to maintain security of their device via password and/or encryption
      - Refer any questions regarding security of patient's device to their cell phone service provider
    - Standard recommendation that in case of emergency the patient should call 911 or go to the nearest hospital
  - Patient consent is educational tool to assure good communications between patient and physician
  - Does not constitute a waiver of patient rights under HIPAA

Steps to Secure e-PHI Texting

1. Complete and document formal risk assessment for texting in your practice
   - Even if you elect not to text - document and **monitor**
2. Protocol allows staff to audit any device used
3. All devices are password protected
   - Check level of security for password
4. Monitor text retention, documentation, deletion policy
5. Devices “purged” prior to discarding

http://www.passwordmeter.com/

LAMMICO

Steps to Secure e-PHI Texting

6. All devices used to text any patient specific data are registered with the practice
7. Train all employees regarding the practice’s texting policy
8. If “non-texting” is your policy stress to employees that texting on private devices data containing patient or business information is strictly prohibited
   - Violation of this policy will subject offending employee to disciplinary actions up to possible termination
   - Enforce policy regardless of offending party

Steps to Secure e-PHI Texting

- Remember that under HIPAA patient has right of access to their PHI and the right to offer an amendment
  - You then make the decision whether to enter the amendment into the patient's medical record
- If you elect not to enter the patient's amendment into the record
  - Document the rationale for your decision
- This holds for any such patient request
  - Text or any other part of patient's record

The Joint Commission and Texting

- The Joint Commission noted that 60% of all reported sentinel events in 2011 were tied to breakdown in communications
- As texting becomes more widespread and customary in healthcare it can be assumed that it too will become part of the solution and/or part of the problem in healthcare communications
- What about texting orders?

The Joint Commission and Texting

- Is it acceptable for physicians and licensed independent practitioners (and other practitioners allowed to write orders) to text orders?
  - **Yes, IF**
    - Secure sign-on process
    - Encrypted messaging
    - Delivery and read receipts
    - Customized message retention time frames
    - Specified contact list for individuals authorized to receive and record orders

https://www.jointcommission.org/update_texting_orders/

LAMMICO

Encryption—Security's Magic Bullet

- As a general HIPAA rule – once data has been encrypted even if the device on which the data is stored is stolen or lost
  - No security breach
  - No reporting
  - No contacting all individuals whose data may have been on the device
- Password protection is good but go one more step
- Device encryption - not required but…

LAMMICO

Encryption—Security's Magic Bullet

- Data protection available for devices that offer hardware encryption such as
  - iPhone 3GS and later
  - All iPad models
  - iPod Touch 3rd generation and later
- Provides an additional layer of protection over mere password protection
- Demonstrates practice's due diligence and good faith effort to secure data on mobile devices

LAMMICO

Encryption—Security's Magic Bullet

- Data protection available for devices that offer hardware encryption such as
  - iPhone 3GS and later
  - All iPad models
  - iPod Touch 3rd generation and later
- The following is an example of such services. It does not constitute a recommendation:

  https://www.quora.com/Are-there-any-Android-devices-that-offer-hardware-encryption-for-data-protection

Other Than HIPAA—Louisiana

- Electronically stored information (ESI) has become a major issue in many high profile legal investigations
- Bottom line for healthcare providers is that all ESI, not just your EMRs, are subject to discovery during a civil (medical malpractice action for example) or criminal (fraudulent billing practices) case
- This would include data stored on personal mobile devices
- Even the anticipation of litigation or investigation
  - Triggers duty to preserve and perhaps produce

LAMMICO

Electronically Stored Information (ESI)

- In addition to mobile devices ESI includes
  - Electronic Medical Records
  - E-mail data
    - Business, personal, whether or not it contains e-PHI
    - Sent or received internal or external to the organization
      - Includes CC’d or copies sent, received or forwarded
  - Any data digitally stored such as videos or photographs
      - Stored on site, offsite, cloud, etc.
  - Digital copies stored on copiers or printers
  - Data stored on hard drives of biomedical devices

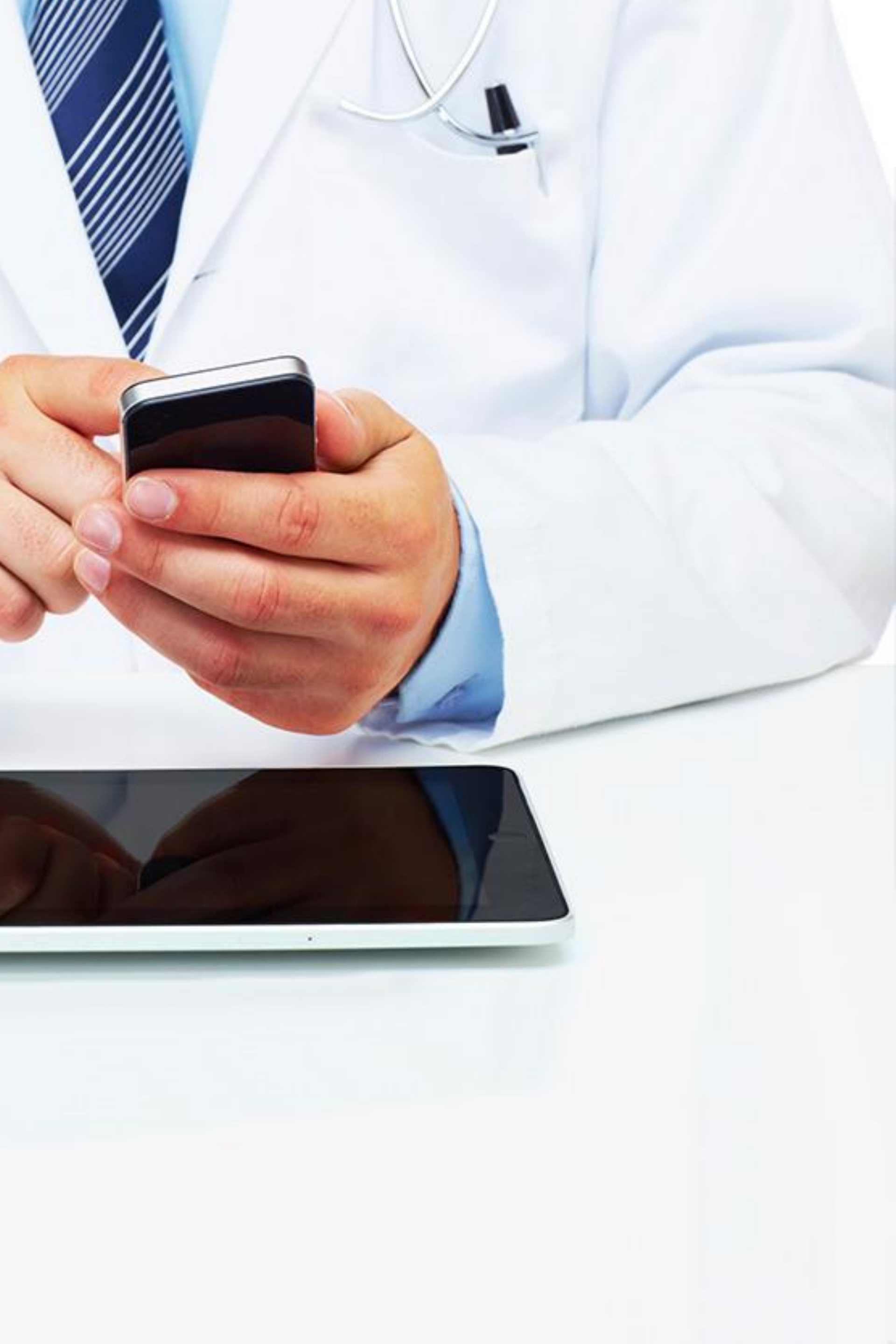
Electronically Stored Information (ESI)

- ESI includes such data as:
  - Back-up data stored on employee's work OR personal computers at remote or home location
  - Back-up "tapes" kept for disaster recovery
  - Archived data regardless of where or how it is maintained
- Failure to preserve and/or produce ESI could be disastrous to a civil or criminal case
- Risk Management Hint: In conjunction with your attorney, develop an ESI Life Cycle Management Policy and make sure it includes cell phones

LAMMICO

Summary

- Both Federal and State law impacts the creation, transmission, storage and access to text messages
- The first step to maintaining privacy and security of any e-PHI is to perform and document a formal risk assessment
  - Implement and monitor procedure(s)
- Always consult your attorney when developing policy and procedures for preservation and production of electronically stored information (ESI)
- Support your office administrator!



Text or Not to Text No Longer the Question

Managing Risk of Medical Texting

James Ronald Kennedy, MHA, MJ, ARM

LAMMICO Risk Management Consultant

LAMMICO