Strafford

Presenting a live 90-minute webinar with interactive Q&A

Portable Electronic Devices in Healthcare: Latest Legal Threat for Providers

Protecting Private Information in Text Messages, Emails and Other Electronic Transmissions

TUESDAY, DECEMBER 11, 2012

1pm Eastern | 12pm Central | 11am Mountain | 10am Pacific

Today's faculty features:

Brian C. Vick, Partner, **Williams Mullen**, Raleigh, N.C.

W. Clifford Mull, **Benesch Friedlander Coplan & Aronoff**, Cleveland

Dianne J. Bourque, Member, **Mintz Levin Cohn Ferris Glovsky and Popeo**, Boston

The audio portion of the conference may be accessed via the telephone or by using your computer's speakers. Please refer to the instructions emailed to registrants for additional information. If you have any questions, please contact **Customer Service at 1-800-926-7926 ext. 10**.

Tips for Optimal Quality

Sound Quality

If you are listening via your computer speakers, please note that the quality of your sound will vary depending on the speed and quality of your internet connection.

If the sound quality is not satisfactory and you are listening via your computer speakers, you may listen via the phone: dial **1-866-370-2805** and enter your PIN when prompted. Otherwise, please **send us a chat** or e-mail **sound@straffordpub.com** immediately so we can address the problem.

If you dialed in and have any difficulties during the call, press *0 for assistance.

Viewing Quality

To maximize your screen, press the F11 key on your keyboard. To exit full screen, press the F11 key again.

Continuing Education Credits

FOR LIVE EVENT ONLY

For CLE purposes, please let us know how many people are listening at your location by completing each of the following steps:

- In the chat box, type (1) your **company name** and (2) the **number of attendees at your location**
- Click the word balloon button to send

WILLIAMS MULLEN

Where Every Client is a Partner®

Recent Trends In The Use Of Mobile Devices In Health Care Settings

Brian C. Vick
919.981.4023
bvick@williamsmullen.com

December 11, 2012

Mobile Device Use Is On The Rise

- 85% of adults in the U.S. own a mobile phone
- 82% use their phone to take pictures
- 80% use their phone to send text messages
- 56% use their phone to access the internet
- 50% use their phone for email
- 44% use their phone to record video
- 43% use their phone to download apps.

** Pew Internet & American Life Project - 2012*

2011 HIMSS Mobile Technology Survey

A survey of 164 hospitals and health systems revealed that mobile devices were being used by:

- 89% of physicians
- 84% of non-physician clinicians
- 70% of healthcare executives
- 62% of administrative / support staff

Clinicians Are Using Mobile Devices To:

- Access non-PHI health information
- View patient information
- Educational / training purposes
- Clinical notifications
- Tracking worklists
- Communicate regarding patients
- Data collection
- Analysis of patient data
- Monitor medical device data

* 2011 HIMSS Mobile Technology Survey, December 5, 2011

The Use Of Mobile Devices In Healthcare Will Increase Dramatically In The Coming Years

- The current push towards quality-based health care delivery systems is increasing the importance of communication and information access
- Mobile access to EMR systems and clinical data will help improve patient safety, reduce medical errors, and increase clinical outcomes
- Remote monitoring and real-time management of chronic diseases (i.e., diabetes, heart disease)
- Physicians are demanding greater mobile access to EMR systems and clinical data
- Studies have shown that mobile devices can improve clinical outcomes by facilitating better patient communications
- Stage 2 Meaningful Use Rules emphasize the importance of electronic communication

But . . . information governance practices surrounding mobile devices have not kept pace with technological developments

HIMSS 2011 Mobile Technology Survey:

- 97% of respondents were using mobile devices of some type
- 77% allowed mobile access over a public network
- 75% allowed mobile access of patient information
- 41% allowed employees to use their own mobile devices
- 38% had a Mobile Technology Policy in place

This Has Lead To Poor Information Governance

- Between 2009 and 2012, hundreds of HIPAA breaches involving mobile devices were reported to HHS

10/10 two USB drives contained PHI on 1469 patients lost by a California hospital

11/10 unencrypted laptop containing PHI on 4486 patients stolen from the home of an employee of a Texas medical practice

2/11 personal laptop containing PHI on 1700 individuals stolen from business associate of Arkansas social services agency in Arkansas

4/11 physician practice in Texas lost unencrypted USB drive containing PHI on 1,105 patients

4/11 unencrypted laptop containing PHI on 1500 patients stolen from Texas hospital

7/12 Alaska Medicaid agrees to pay HHS $1.7 million to resolve HIPAA breach after portable hard drive containing PHI was stolen from employee's car

9/12 Massachusetts practice agrees to pay HHS $1.5 million to settle HIPAA breach based on inadequate management of PHI on mobile devices

Mobile Device Misuse Is Also On The Rise

- California 2007 — 9 hospital employees fired for taking or looking at cellphone pictures of patient x-rays
- Wisconsin 2009 — Nurse fired for posting a cell-phone picture of a patient x-ray on Facebook
- Oregon 2012 — Nurse sentenced to 8 days in jail after posting “disturbing” photos of elderly patients on Facebook
- California 2012 — 5 nurses fired for discussing patients on Facebook

Portable Electronic Devices in Healthcare: Latest Legal Threat for Providers : Legal Risks for Hospitals and Providers

December 11, 2012

W. Clifford Mull

Benesch, Friedlander, Coplan & Aronoff LLP

200 Public Square, Suite 2300

Cleveland, OH 44114-2378

Direct: 216.363.4198 | Fax: 216.363.4588 | Mobile: 216.287.9940

cmull@beneschlaw.com | www.beneschlaw.com | www.beneschhealthlaw.com

Legal Risks

- Introduction
  - Patient Privacy
  - Professional Liability

Patient Privacy: HIPAA Privacy and Security Regulations

- **Generally**. Covered Entities required to protect ePHI that they use or disclose to business associates, trading partners, or other entities.
  - Covered Entities. Health Plans, Health Care Clearinghouses, and Health Care Providers.

Patient Privacy: HIPAA Privacy and Security Regulations

- **Privacy Requirements**. Require Covered Entities to limit uses and disclosures of PHI, to employ administrative measures to protect PHI and to document compliance.
- **Security Requirements**. Require Covered Entities to adopt and implement appropriate administrative, technical and physical safeguards that:
  - Ensure the confidentiality, integrity and availability of ePHI ;
  - Protect against reasonably anticipated threats or hazards to the security or integrity of ePHI;
  - Protect against reasonably anticipated uses or disclosures of ePHI not permitted by the Privacy Rule; and
  - Ensure compliance with all such protection by the Covered Entity's workforce.

Patient Privacy: Policies and Procedures Identified by OCR for Portable Devices

- Develop and Implement Policies and Procedures Authorizing ePHI Access
- Develop and Implement Policies and Procedures to protected ePHI stored on remote or portable devices or on potentially transportable media
- Develop and implement appropriate policies and procedures to secure ePHI that is being transmitted over an electronic communications network

Patient Privacy: HIPAA Breach Notification Requirements

- Covered Entities are required to report breaches of unsecured PHI to all affected individuals, federal regulators, and, under certain circumstances, the media.
  - **"Unsecured PHI."** PHI that is not secured using technology or methodology that renders it unusable, unreadable or indecipherable by unauthorized individuals.
  - **"Breach."** The access, use or disclosure of PHI in a manner not permitted by the Privacy Rule which compromises the PHI's security or privacy.
  - **"Media Notification."** Breaches affecting more than 500 residents of the State or jurisdiction.

Patient Privacy: Penalties for Violations

- **Civil Monetary Penalties**.
  - Did not know and, exercising reasonable diligence, would not have known of violation, then civil monetary penalty by cannot be:
    - less than $100 per violation; and
    - more than: (i) $50,000 per violation or (ii) $1,500,000 per calendar year for identical violations.
  - Violation due to reasonable cause and not willful neglect, then the civil monetary penalty cannot be:
    - less than $1000 per violation; or
    - more than: (i) $50,000 per violation; or (ii) $1,500,000 per calendar year for identical violations.

Patient Privacy: Penalties for Violations continued

- **Civil Monetary Penalties Continued**.
  - Violation due to willful neglect but is corrected within 30 days of the covered entity knowing, or exercising reasonable diligence, when the covered entity would have known of the violation, then the civil monetary penalty cannot be:
    - less than $10,00 per violation; or
    - more than: (i) $50,000 per violation; or (ii) $1,500,000 per calendar year for identical violations.
  - Violation due to willful neglect but is not corrected within 30 days, then the civil monetary penalty cannot be:
    - less than $50,000 per violation; or
    - more than $1,500,000 per calendar year for identical violations.
- **State AG Enforcement.**

Patient Privacy: Risk Areas Identified by OCR for Portable Electronic Devices and Overview of Reported Breaches

"New standards and technologies have significantly simplified the way in which data is transmitted throughout the healthcare industry and created tremendous opportunities for improvements to the healthcare system. However, these technologies have also created complications and increased the risk of loss and unauthorized use and disclosure of this sensitive information." *OCR HIPAA Security Guidance for Laptops, Other Portable and/or Mobile Devices and External Hardware.*

Patient Privacy: Risk Areas Identified by OCR for Portable Electronic Devices and Overview of Reported Breaches

- **Accessing ePHI (Unauthorized Access)**
  - Log-in Credentials Lost or Stolen
  - Unauthorized Access Offsite
  - Unattended Offsite Workstation
  - Introduction of Virus through External Device used for Remote Access

Patient Privacy: Risk Areas Identified by OCR for Portable Electronic Devices and Overview of Reported Breaches

- **Storing ePHI**
  - Portable Device Lost or Stolen
  - Loss of Operationally Critical ePHI on remote device
  - Inappropriate Disposal of Portable Device
  - Data Left on Third Party External Device
  - Introduction of Virus through Portable Storage Device

Patient Privacy: Risk Areas Identified by OCR for Portable Electronic Devices and Overview of Reported Breaches

- **Transmitting ePHI (Integrity and Safety)**
  - Interception or Modification of Data during Transmission
  - Introduction of Virus from External Transmission Device

Patient Privacy: Recent HIPAA Settlements

- **Alaska Department of Health and Social Services (June 2012)**
  - $1.7 Million Settlement
  - Lost USB hard drive

Patient Privacy: Recent HIPAA Settlements

- **Blue Cross Blue Shield of Tennessee (March 2012)**
  - $1.5 Million Settlement
  - Loss of Computer Hard Drives

Patient Privacy: Recent HIPAA Settlements

- **Massachusetts Eye and Ear Infirmary and Massachucetts Eye and Ear Associates (September 2012)**
  - $1.5 Million Settlement
  - Theft of Personal Laptop

Patient Privacy: Recent HIPAA Settlements

- **Providence Health & Services (July 2008)**
  - $100K Settlement
  - Lost or stolen backup tapes, optical disks, and laptops

Professional Liability

- Distraction of Health Care Professionals
- Cyber Liability
- Defamation and Other State Invasion of Privacy

MINTZ LEVIN
Mintz Levin Cohn Ferris Glovsky and Popeo PC

Portable Electronic Devices in Healthcare: Latest Legal Threat for Providers

Protecting Private Information in Text Messages, Emails and Other Electronic Transmissions

December 11, 2012

BYOD and RISK MANAGEMENT

Dianne J. Bourque, Esq.

Portable devices offer a variety of benefits to covered entities and business associates alike. A deliberate and well-planned approach is the key to minimizing the risks associated with BYOD.

Risk Assessment

- A comprehensive risk assessment is the first step in managing a BYOD program
  - It may reveal that employees are already using their own devices and associated risks to PHI
  - It may reveal that BYOD is technically or financially infeasible for your organization
- If BYOD is feasible, a risk assessment will help you to identify the best technical means for program impelementation
- Risk assessment findings will also support the development of BYOD policies and procedures
- A risk assessment will demonstrate HIPAA compliance in the event of an OCR audit or investigation

Risk Assessment, continued

- Your risk assessment should include:
  - Documentation of the risks associated with devices outside of your control
  - Documentation of applications and resources potentially exposed by individuals using their own devices
  - Documentation of technology solutions to facilitate BYOD (make sure that the solutions address identified risks)

Policies and Procedures

- Once your risk assessment is complete and your organization has selected the best technical approach for program implementation, written policies and procedures should be developed governing BYOD.
- Policies and procedures should define:
  - How mobile devices support the overall mission and business goals of your organization.
  - What type/s of mobile devices your organization will support
  - Which classes of employees will be permitted to use mobile devices for business purposes
  - Which classes of employees will be permitted to store or transmit ePHI locally on a device and how such data will be encrypted

Policies and Procedures, continued

- Policies and procedures should include notice to employees that violations of the company's BYOD policies may result in disciplinary action and/or the loss of the privilege of using a personal device for business purposes

Employee Agreement

- Policies and procedures ought to include a written agreement to be signed by the employee acknowledging conditions for participation in the BYOD program. The agreement would memorialize the employee's agreement to:
  - Install, update and administer security software
  - Remotely wipe or lock the device if lost or stolen
  - Abide by the company's data access, use and other security measures

Training

- The key to any successful security program is training
- Regular, formal training and informal reminders are equally critical for maintaining a culture of compliance
- Practical training, with real-life examples is most effective
- Don't forget to document training in order to demonstrate compliance in the event of audit or investigation

Thank you !

Dianne J. Bourque, Esq.
Mintz, Levin, Cohn, Ferris, Glovsky and Popeo, P.C.
One Financial Center
Boston, MA 02111
(617) 348-1614 / DBourque@mintz.com