Ensuring HIPAA Compliance When Transmitting PHI Via Patient Portals, Email and Texting

Protecting Patient Privacy, Complying with State and Federal Regulations, and Meeting Meaningful Use Stage 2 Standards

WEDNESDAY, JUNE 18, 2014

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

Today’s faculty features:

Ryan P. Blaney, Member, Cozen O’Connor, Washington, D.C.

Diane M. Welsh, Shareholder, von Briesen & Roper, Madison, Wis.

Christy Navarro, Principal Consultant, Navarro Consulting, Sacramento, Calif.

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, you may listen via the phone: dial 1-866-869-6667 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 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 SEND button beside the box

If you have purchased Strafford CLE processing services, you must confirm your participation by completing and submitting an Official Record of Attendance (CLE Form).

You may obtain your CLE form by going to the program page and selecting the appropriate form in the PROGRAM MATERIALS box at the top right corner.

If you'd like to purchase CLE credit processing, it is available for a fee. For additional information about CLE credit processing, go to our website or call us at 1-800-926-7926 ext. 35.
If you have not printed the conference materials for this program, please complete the following steps:

- Click on the ^ symbol next to “Conference Materials” in the middle of the left-hand column on your screen.
- Click on the tab labeled “Handouts” that appears, and there you will see a PDF of the slides for today’s program.
- Double click on the PDF and a separate page will open.
- Print the slides by clicking on the printer icon.
Ensuring HIPAA Compliance When Transmitting PHI Via Patient Portals, Email and Texting

June 18, 2014

Ryan P. Blaney, Esq.
Cozen O'Connor, Washington, DC
rblaney@cozen.com
(202) 463-2528

Christy Navarro, Principal Consultant
Navarro Consulting, Sacramento, CA
cnavarro@navarroprivacy.com
(916) 541-7404

Diane M. Welsh, Esq.
von Briesen & Roper, Madison, WI
dwelsh@vonbriesen.com
(608) 661-3961

Sponsored by the Legal Publishing Group of Strafford Publications
OVERVIEW OF PRESENTATION

Introduction & State of the Industry
- ACA and Meaningful Use Stage 2
- Patient Portals – What are they?
- Consumer driven healthcare – Access
- Lifecycle of Patient Portal

Patient Portal Design & Contracting
- Scope and Scale
- Access and Control
- Contracting with Patient Portal Vendors
- Business Associate Agreements

Patient Portal Use & Safeguards
- Training of Workforce
- Policies and Procedures
- Enforcement and Monitoring
- Minimum Necessary

Patient Portals – Pitfalls
- Technical & Legal Issues
- Access – parents, guardians, seniors
- Audits by HHS
- Post Portal Implementation and Termination
Health Care Reform & Financial Incentives

• Health Information Technology for Economic and Clinical Health (HITECH) Act
  – Incentive payments to providers who employ “meaningful use” of certified EHR technology.
  – Beginning in 2015, Medicare (but not Medicaid) will reduce payments to physicians and other providers who are eligible but choose not to participate.
Meaningful Use Measures

• Patient portals are a way to meet the meaningful use requirements ("measures")
  - **Core measures** - i.e., providing patients with an electronic copy of their health information; providing clinical summaries for each office visit
  - **Menu measures** – i.e., providing patients with timely electronic access to their health information; patient-specific education resources
What is a Patient Portal?

- A secure online website that gives you 24-hour access to your personal health information and medical records.
Consumer-focused Health Care???
Facts & Stats

U.S. Consumers Willing to Change Doctors to Gain Access to Electronic Medical Records

Virtually All
98% say they should have at least some access online to their medical records

Many Consumers
2 in 5 willing to change doctors to gain access to electronic medical records

U.S. Consumers
Current access to healthcare IT

48% can request refills online
43% can schedule appointments online
38% receive reminders via email or text message
43% can access their electronic records

Source: Accenture consumer health survey, 2013
Patient Interaction & Partnership

• 84% of US consumers with smart phones/home computers – want access to electronic medical records
• 41% willing to switch doctors over issue
• 70% of consumers believe its important to be able to consult their providers via email.

Lifecycle of Patient Web Portal

- Contracting with vendors
- Portal Design
- Use and Safeguards
- Post Implementation and Termination
Patient Web Portal – Selecting & Design Phase

• **Evaluating Patient Portal Vendors**
  – Secure messaging with providers?
  – Do they have a privacy & security officer(s)?
  – Proxy Access?
  – Portal maintenance and repairs

• **Design phase**
  – Security, access and control
  – Mobile friendly
Contracting

• Don’t just sign the standard contract placed in front of you!
• Pay attention to clauses/provisions:
  – Who owns the data?
  – Term and renewal
  – Indemnification
  – Limitations on Liability
  – Reporting requirements and breaches
  – Termination and data (discussed later)
What is a Business Associate ("BA")?

• Definition:
  – A person who (i) performs for or on behalf of a covered entity, or assists
    a covered entity, in performing an activity or function involving use or
    disclosure of health information (e.g., claims processing, utilization
    review, billing), or (ii) provides legal, actuarial, accounting,
    management, administrative, accreditation or financial services where
    the provision of such services involves the disclosure of health
    information from the entity or another business associate of the entity

• Includes anyone with health information from your
  health plans, providers and covered entities (could
  include attorneys, consultants, third party
  administrators, auditors, computer software service
  companies)
HHS published a Final Omnibus Rule on January 25, 2013 that expanded the definition of Business Associates to include Health Information Organizations, E-prescribing Gateways, entities that provide data transmission services for PHI and who require routine access to such PHI, and personal health record vendors.
What are the Business Associate Rules?

- General Rules
  - Need specific HIPAA-dictated language in a contract with all business associates
  - Business Associate Agreement must be written.
  - Must include language that specifically says that the BA will ensure that individual’s HIPAA rights are followed.
Continued …

• Under HITECH all of the HIPAA rules apply directly to business associates, including penalties
  
  – Previously, HIPAA applied only to “covered entities” – health plans, health care providers, and clearinghouses
  
  – HIPAA applied indirectly to business associates – through business associate agreements
Tips for Drafting & Negotiating BAAs

• Reporting requirements and timing (the parties can and should agree on shorter periods)
• Review the underlying services agreement and modify services agreement and BAA to be consistent
• Agency and subcontractor provisions
• Indemnification clauses
• Breach notification costs and responsibilities
• Termination and destruction of PHI
Patient Portal Use and Safeguards

Diane M. Welsh
Promoting Use

• **Identify Physician Champions.** Identify physician champions to lead by example.

• **Training.** Conduct standardized in-service training to all employees.

• **Support.** Trainers and clinic-based super-users provide hands-on support as needed.

• **Inform and Encourage Patients.** Providers and staff inform patients of availability and advantages of portal and encourage participation. Promote use of portal through other channels, as well (newsletters, local media).

adapted from: http://www.healthit.gov/providers-professionals/patients-first-health-care-case-study
Want to Ask Your Doctor a Question Any Time, Any Where?

Join our FREE Patient Website and securely email your doctor online any time of the day!
- Request or Change Appointments
- Safely Email Your Doctor
- View Lab Results
- Request Prescription Refills
- View Medical Records

Sign Up Today!
For more information ask the front desk or go to www.portalname.com.

Requesting Your Appointment Has Never Been So Easy

Connect to our FREE patient website. It’s fast, easy and you never have to listen to on hold music again!
- Request or Change Appointments
- Safely Email Your Doctor
- View Lab Results
- Request Prescription Refills
- View Medical Records

Sign Up Today!
For more information ask the front desk or go to www.portalname.com.
Disclaimers for Patients

- Never Use for Urgent Messages
  - Message Response Time

- Password Management
  - Keep Passwords Confidential
  - Changing Password

- Use Portal, not unsecured email, for Secure Communication with Provider
Workforce Training

• HIPAA training, when hired and annually

• Portal-specific training
  - To ensure proper use by workforce
  - So workforce can properly assist patients
  - Avoids improper or riskier means of communication
Policies and Procedures

• Protocols for Transmitting Information to Patients in a Patient-Centered, Timely Manner

• Secure Messages to Patients

• Considerations for Adolescent Patients

• Caregiver Access

• Incident Reports

• Deactivating Accounts
Minimum Necessary Standard

• Covered Entities must make reasonable efforts not to use or disclose more than the minimum amount of health information necessary to accomplish the intended purpose of the disclosure

• With limited exceptions, the standard generally applies to all uses and disclosures of health information

45 CFR § 164.502(b)
Minimum Necessary Exceptions

Standard does not apply to:

- Disclosures to a health care provider for treatment purposes
- Authorized uses or disclosures
- Disclosures for HIPAA compliance purposes (e.g., most disclosures to HHS)
- Uses or disclosures that are required by law and specifically permitted in the Privacy Rule without individual authorization
Security Rule Requirements

• Ensure confidentiality, integrity, and availability of ePHI

• Protect against reasonably foreseeable threats to the security or integrity of ePHI

• Protect against reasonably anticipated uses or disclosures of ePHI that are not permitted by Privacy Rule

45 CFR § 164.306(a)
<table>
<thead>
<tr>
<th>Security Components</th>
<th>Examples</th>
<th>Examples of Security Measures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical Safeguards</td>
<td>• Your facility and other places where patient data is accessed</td>
<td>• Building alarm systems</td>
</tr>
<tr>
<td></td>
<td>• Computer equipment</td>
<td>• Locked offices</td>
</tr>
<tr>
<td></td>
<td>• Portable devices</td>
<td>• Screens shielded from secondary viewers</td>
</tr>
<tr>
<td>Administrative Safeguards</td>
<td>• Designated security officer</td>
<td>• Staff training</td>
</tr>
<tr>
<td></td>
<td>• Workforce training and oversight</td>
<td>• Monthly review of user activities</td>
</tr>
<tr>
<td></td>
<td>• Controlling information access</td>
<td>• Policy enforcement</td>
</tr>
<tr>
<td></td>
<td>• Periodic security reassessment</td>
<td></td>
</tr>
<tr>
<td>Technical Safeguards</td>
<td>• Controls on access to EHR</td>
<td>• Secure passwords</td>
</tr>
<tr>
<td></td>
<td>• Use of audit logs to monitor users and other EHR activities</td>
<td>• Backing-up data</td>
</tr>
<tr>
<td></td>
<td>• Measures that keep electronic patient data from improper changes</td>
<td>• Virus checks</td>
</tr>
<tr>
<td></td>
<td>• Secure, authorized electronic exchanges of patient information</td>
<td>• Data encryption</td>
</tr>
<tr>
<td>Policies &amp; Procedures</td>
<td>• Written policies and procedures to assure HIPAA security compliance</td>
<td>• Written protocols on authorizing users</td>
</tr>
<tr>
<td></td>
<td>• Documentation of security measures</td>
<td>• Record retention</td>
</tr>
<tr>
<td>Organizational Requirements</td>
<td>• Breach notification and associated policies</td>
<td>• Agreement review and updates</td>
</tr>
<tr>
<td></td>
<td>• Business associate agreements</td>
<td></td>
</tr>
</tbody>
</table>
Security Risk Analysis Process

1. Review existing security of protected health information
2. Identify threats and vulnerabilities
3. Mitigate security risks
4. Assess risks for likelihood and impact

Monitor results
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 the Security Risk Assessment Tool (SRAT).

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.

http://www.healthit.gov/providers-professionals/security-risk-assessment
Security Rule: Access Control

The Security Rule defines access in § 164.304 as “the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource.”

Access controls provide users with rights and privileges to access and perform functions using information systems, applications, programs, or files. Access controls should enable authorized users to access the minimum necessary information needed to perform job functions. Rights or privileges should be granted to authorized users based on a set of access rules that the covered entity is required to implement as part of § 164.308(a)(4), the Information Access Management standard under the Administrative Safeguards section of the Rule.

The Access Control standard requires a covered entity to:

“Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4)[Information Access Management].”
Access Control

- A covered entity can comply with this standard through a combination of access control methods and technical controls.

- There are a variety of access control methods and technical controls that are available within most information systems. The Security Rule does not identify a specific type of access control method or technology to implement.

- Access controls should be appropriate for the role and function of the workforce member.

- Four implementation specifications are associated with the Access Controls standard.
  1. Unique User Identification (Required)
  2. Emergency Access Procedure (Required)
  3. Automatic Logoff (Addressable)
  4. Encryption and Decryption (Addressable)
Security Rule: Authentication

Must: “Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.”

In order to determine which electronic mechanisms to implement to ensure that electronic PHI is not altered or destroyed in an unauthorized manner, a covered entity must consider the various risks to the integrity of the electronic PHI identified during the risk analysis.

After covered entities have identified risks to the integrity of the data, they must identify security measures that will reduce the risks.
Security Rule: Audit Controls

The Audit Controls standard requires a covered entity to:

“Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.”

Most information systems provide some level of audit controls with a reporting method, such as audit reports. These controls are useful for recording and examining information system activity, especially when determining if a security violation occurred.

The Security Rule does not identify data that must be gathered by the audit controls or how often the audit reports should be reviewed.

A covered entity must consider its risk analysis and organizational factors, such as current technical infrastructure, hardware and software security capabilities, to determine reasonable and appropriate audit controls for information systems that contain or use electronic PHI.
Audit Controls

Consider:
What audit control mechanisms are reasonable and appropriate to implement so as to record and examine activity in the patient portal?

What are the audit control capabilities of the patient portal?

Do the audit controls implemented allow the organization to adhere to policy and procedures developed to comply with the required implementation specification for Information System Activity Review?
Avoiding Legal & Technical Pitfalls

Christy Navarro, MS, CIPP/US
Risk Areas to Evaluate

- Multi-State Deployment
- Infants
- Minors (age 12-17)
- Release of Lab Results Timing
- PHI Requiring Additional Protections
- Accepting Patient Payments via the Portal
Additional Considerations

- Notice of Privacy Practices
- Integrity Controls & Audit Log Capability
- Detecting and Preventing Breaches
- Leverage Portal for Other HIPAA related Requests
- Don’t annoy the patients with cumbersome requirements
Practical Steps to Reduce Risk

1. Create Data Sets
2. Soft Go-Live
3. Written Procedures
4. Training on Procedures
Practical Steps to Reduce Risk Cont.

Right Patient, Right Information

Help Desk for Patients

Meaningful Use

Assign Internal Ownership

Navarro Consulting
Data Privacy and Health Informatics Expertise
Audits by HHS and OCR

“HIPAA Compliance is like middle school math – you must show your work”

– Leon Rodriguez, Director Office of Civil Rights

• HIPAA related recordkeeping is essential.
• Audit: Leverage OCR’s HIPAA Privacy, Security and Breach Audit Protocol available online.
• Assessments: analysis of vulnerabilities, data criticality, remediation strategies and process for determining and accepting risks in the organization.
HITECH’s New ‘Objective’ Method for Assessing Breaches

The Omnibus Rule made significant changes to the interim final breach notification rule by:

• Adding a *presumption* that any unauthorized use or disclosure of unsecured PHI is a breach

• Removing the prior “risk of harm“ standard.

• Requires Covered Entities to evaluate and demonstrate that “low probability” PHI has been “compromised” otherwise notification to patients required
# Enforcement Penalties

<table>
<thead>
<tr>
<th>Violation Category</th>
<th>Each Violation</th>
<th>Year Cap for Same Violation</th>
</tr>
</thead>
<tbody>
<tr>
<td>(A) Did not know</td>
<td>$100-$50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>(B) Reasonable Cause</td>
<td>$1,000-$50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>(C) Willful Neglect – Corrected</td>
<td>$10,000-$50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>(D) Willful Neglect – Not Corrected</td>
<td>$50,000</td>
<td>$1,500,000</td>
</tr>
</tbody>
</table>
Breaches and Reporting

• Consider state law obligations as well as federal
• Include in contract:
  • Contact information in the event of an “incident” – define “incident”
  • Will the vendor determine if something is a breach or simply report “incidents” so the CE can evaluate
• Does your portal vendor have a privacy officer?

*CE’s have more experience in the nuances of evaluating if a “Breach” has occurred.*
Post Portal Implementation

- Budget for ongoing support and maintenance
- Project Documentation (recordkeeping)
- Fully incorporate into existing Privacy & Data Security Program
Changing Vendors

**Previous Vendor**
- Arrange return or destruction of PHI
- Review contract
- Former patient portal web address

**New Vendor**
- Leverage existing patient portal infrastructure
- Perform a gap analysis
- Remediate gaps
- Incorporate lessons learned
Shutting Down A Patient Portal

Data Retention Requirements

Return or destruction of PHI

Former patient portal web address
Handout Available

Patient Portal Vendor Checklist: *Important Privacy and Security Questions to Ask a Vendor before Signing on the Dotted Line*