manatt

HIPAA and Emerging Technologies: Protecting Privacy When Communicating in the Digital Age

June 6, 2017

Presenter Information

Jill DeGraff Thorpe, JD

Partner, Manatt Health

Helen Pfister, JD

Partner, Manatt Health

Randi Seigel, JD

Counsel, Manatt Health

Introduction

Technology is transforming the way medical professionals communicate and coordinate care. How do we keep this convenience from compromising patient privacy or increasing organizational exposure?

New Technologies. The complexity of managing these risks is heightened by the continued emergence of new technologies, the transition by the health care industry to established forms of mobile communications and the increased reliance on tech vendors offering cloud-based services.

User Expectations. All of these technologies help HIPAA-covered entities move towards meeting patient expectations for relevant, consumable content, ready access to their health information and convenient communications with their care teams.

Optimizing Workflows. These technologies can also alleviate administrative burdens, generate efficiencies and enable geographically dispersed care teams to coordinate care better.

Objectives

- Understanding the advantages and disadvantages/risks of using digital tools to optimize communications and organizational workflow while mitigating HIPAA risk
- Identify the qualities to look for when choosing vendors and platforms to enable health-related communications while ensuring HIPAA compliance
- Explore how to provide ongoing oversight to protect your organization after vendors and platforms have been deployed
- Reveal how to avoid common HIPAA traps that organizations fall into when using new technologies

Agenda

- Enforcement Landscape
- Selected HIPAA Rules
- Communication Technologies
  - Portals
  - Email
  - BYOD
  - Texting
  - Mobile Apps
  - IoT
- Evaluating and Contracting with Vendors
- Review of Compliance Strategies

President Trump believes cybersecurity is a priority: budget blueprint allocates $1.5 billion for the Department of Homeland Security for this purpose.*

HHS Secretary Tom Price: “Rules of the road” are needed to achieve “true interoperability”.

Vulnerability to cyberthreats is a priority. In April, HHS announced that it would be establishing a center modeled after the Homeland Security Department’s National Cybersecurity and Communications Integration Center to assess cyberthreats and deliver best practices to smaller health care practices and mobile app developers.

Roger Severino, the new Director for the HHS Office of Civil Rights (OCR), declared that his office’s enforcement actions would adapt to new data security threats, including those raised by ransomware, interoperability and mobile apps.

* source: http://thehill.com/policy/cybersecurity/324238-trumps-budget-proposal-gives-dhs-15-billion-for-cybersecurity

Phase 2 audits continue.

Weaknesses Identified in Phase 1

- Risk analysis and risk management
- Content and timeliness of breach notifications
- Notice of privacy practices
- Individual access
- Privacy standards/reasonable safeguards requirements
- Training
- Device/media controls
- Transmission security

Phase 2 Additional Focus Areas

- Inventory of devices and other information system assets
- Evidence of IS audit logs, access reports and security incident tracking
- Inventory of business associates

Desk audits for select business associates are expected to begin by late 2017 or early 2018, after covered entity site visits are completed.

OCR Investigations

- The OCR investigates complaints it receives of alleged HIPAA violations
- Investigations lead to a **review of pertinent policies, procedures or practices** of the covered entity or business associate and the circumstances regarding the alleged violation
- OCR will take regulatory action if the facts indicate a possible violation due to **willful neglect**

Civil Money Penalties

- Tied to number of violations. OCR can use statistical sampling to establish its prima facie case of the number of violations

Minimum Penalty

- $100—no knowledge or, by exercising reasonable diligence, would not have known of the violation
- $1,000—reasonable cause but not willful neglect
- $10,000—willful neglect but corrected within 30 days of knowing

Maximum Penalty

- Up to $50,000 per violation
- Capped at $1.5M annually for each identical violation
- Each day is a new violation

- Examples of aggravating or mitigating factors:
  - How many individuals affected
  - Length of time the violation continued
  - Nature of the harm (physical, financial, reputational)
  - History of prior compliance
  - Size of the covered entity or business associate

Use Case: CardioNet

In 2012, CardioNet notified OCR that a laptop holding PHI from approximately 1,300 individuals was stolen from an employee's parked car.

- **Findings from ensuing investigation**
  - Unable to remote wipe or disable the stolen device
  - Failed to conduct an accurate and thorough risk analysis
  - Failed to implement security management process
  - No policy or procedures for securing devices or media controls
  - Policies and procedures in draft form, and not yet implemented

- **Agreed to $2.5M civil money penalty and 2-year Corrective Action Plan**
  - Conduct a risk analysis, for the OCR's approval
  - Promptly update Risk Analysis in response to environmental or operational changes affecting the security of ePHI
  - Review the risk analysis at least annually
  - Develop and implement a Risk Management Plan, for the OCR's approval
  - Revise its Security Rule training program, for the OCR's approval, and conduct the training
  - Notify regulators of any employee's failure to comply with the Policies and Procedures

Announcing the settlement, Mr. Severino made clear that mobile apps are going to be intensely scrutinized by OCR in the years ahead.

More OCR Enforcement Actions

- *April 20, 2017*: OCR settled with a small pediatric practice for failure to enter into a business associates agreement with FileFax, Inc., which stored records containing PHI for the entity
- *January 18, 2017*: MAPFRE paid $2.2M to settle allegations that it failed to conduct a risk analysis, implement risk management plans or use encryption on its removable storage media, after a USB device containing ePHI was stolen
- *September 23, 2016*: CNE, a business associate, settled for $400K for not having an updated BAA with its parent company, Woman & Infants Hospital
- *August 4, 2016*: Advocate Health Care settled for $5.55M due to a data breach affecting 4M individuals. OCR uncovered that Advocate had not conducted a risk assessment, implemented P&Ps, or entered into BAAs with key BAs
- *March 16, 2016*: North Memorial Health Care of Minnesota agreed to pay $1.5M to settle allegations that it failed to enter into a BAA with a major contractor and failed to institute a risk analysis to address the risks and vulnerabilities to its ePHI

Worse Than OCR – Cyberattacks

- In 2015, records of about 100M patients were compromised by cyberattacks against health care organizations
- Major Drivers
  - **High-Value Data.** PHI includes immutable identifiers (DoB and SSN) that make medical record data more reliable than credit card information
  - **Vulnerable Industry Sector**. As a whole, healthcare invests less in cybersecurity than other industry sectors
- In May 2017, a global ransomware attack infected tens of thousands of computers, in approximately 100 countries, including the US and the UK
- In April and May 2017, several hospitals in the US were attacked by ransomware that prevented health care providers from accessing patient files
  - The threat to patient safety makes providers especially vulnerable to ransomware attacks

Agenda

- Enforcement Landscape
- Selected HIPAA Rules
- Communication Technologies
  - Portals
  - Email
  - BYOD
  - Texting
  - Mobile Apps
  - IoT
- Evaluating and Contracting with Vendors
- Review of Compliance Strategies

Common Terms

- **PHI**. Any individually identifiable health information that is transmitted or maintained in any form or medium by a covered entity.
  - Limited data sets
  - De-identified information

- **Covered Entities**. Health care providers, health plans and health care clearinghouses.

- **Business Associates**. An organization that creates, receives, maintains or transmits PHI on behalf of a covered entity for functions under the HIPAA rule, or that provides certain services to a covered entity.

Tech Vendors Are Business Associates

- **Business Associate** – Any tech vendor that creates, receives, maintains or transmits PHI on behalf of a covered entity for functions under the HIPAA rule will in most cases be considered to be business associates
- **Downstream vendors** – Any service provider to the tech vendor that creates, receives, maintains or transmits the covered entity's PHI on behalf of the tech vendor is a business associate
  - **Mere Conduit Exception** – Electronic equivalent of a courier where access to ePHI is transient (not persistent) are not business associates. Temporary storage incident to transmission.

Does exception apply to:	
Broadband providers	Yes
Cellular carriers	Yes
Email services	No
Commercial messaging platforms	No
Mobile app developer	Depends

Security Rule



Standards for Safeguarding PHI	Administrative	Physical	Technical
	▪ Security management ▪ Assigned responsibility ▪ Workforce security ▪ Training ▪ Incident procedures ▪ Contingencies ▪ Updates	▪ Facility access ▪ Workstation controls ▪ Device and media controls ▪ Accountability ▪ Backup and storage	▪ Access control ▪ Audit controls ▪ Integrity ▪ Access authentication ▪ Transmission security
Implementation Specifications			
Required	Risk analysis	Disposal of electronic devices	Unique user IDs
Addressable	Log-in monitoring	Data backup	In-transit encryption

- With appropriate documentation, “addressable” specs need not be implemented
- Several factors to consider regarding flexibility in approach to implementing security measures

Organizational Requirements

- Reasonable and appropriate policies and procedures in writing, reviewed and updated periodically in response to environmental or operational changes
- Maintain a written record of any action, activity or assessment required by the Security Rule
- Business associate agreements with business associates
- 6 year document retention

Breach Notification Rule

- OCR presumes that loss of unencrypted data is reportable breach
- Breach notification policy in place that accurately reflects the content and deadline requirements for breach notification
  - "Discovery" is made on the first day a breach is known to the covered entity, or by exercising reasonable diligence, would have been known to the covered entity
  - Any unauthorized use or disclosure of unsecured PHI is presumed to be a breach
  - Shifts burden to covered entity to evaluate and demonstrate that there is a low probability that PHI has been compromised

Privacy Rule

Permitted Uses and Disclosures of PHI

- Treatment, payment and health care operations
- Opportunity to agree or object
- Public purpose disclosures
- Limited data set (16 identifiers)
- De-identified data (19 identifiers)
- With authorization

Administrative Safeguards

- Notice of privacy practices
- Minimum necessary
- Business associates

Rights of Individuals

- Privacy protection
- Access to designated record set
- Accounting of disclosures
- Request of records

Restrictions on Use and Disclosure

- Marketing
- Genetic information
- Psychotherapy notes
- Obtained under a promise of confidentiality
- Risk of substantial harm to patient or other person

Agenda

- Enforcement Landscape
- Selected HIPAA Rules
- Communication Technologies
  - Portals
  - Email
  - BYOD
  - Texting
  - Mobile Apps
  - IoT
- Evaluating and Contracting with Vendors
- Review of Compliance Strategies

Common Issues Encountered by Covered Entities

- Patient preferences
- Dispersed workforce
- BYOD
- Device management
- Adapting policies/procedures to dynamic mobile technology environment
- Data use and sharing
- Tech vendor compliance

Agenda

- Enforcement Landscape
- Selected HIPAA Rules
- Communication Technologies
  - Portals
  - Email
  - BYOD
  - Texting
  - Mobile Apps
  - IoT
- Evaluating and Contracting with Vendors
- Review of Compliance Strategies

Portals

Portals | Email | BYOD | Texting | Apps | IoT

Advantages

- User authentication
- Terms of Service
- Privacy Notice
- Content Controls
- Minimum Necessary
- Data Use
- Record Access
- Meaningful Use and MACRA

Disadvantages/Risk Factors

- Patients slow to adopt
- Implementation costs are high
- Complex implementation tends to discourage innovation

Practice Tips:

- Policies for patient portals are a good starting point

Agenda

- Enforcement Landscape
- Selected HIPAA Rules
- Communication Technologies
  - Portals
  - Email
  - BYOD
  - Texting
  - Mobile Apps
  - IoT
- Evaluating and Contracting with Vendors
- Review of Compliance Strategies

Email

Portals | **Email** | BYOD | Texting | Apps | IoT

Advantages

- Easy adoption
- Can be uploaded to EHR
- Able to be encrypted
- Patients can consent to receive unencrypted emails

Disadvantages/Risk Factors

- User authentication
- Transmission security
- Integrity control
- Accountability
- Servers may reside outside of the U.S.
- Multiple instances of email on the internet

Practice Tips:

- Obtain patient consent
- Use fax/phone and portal policies/procedures for guidance
- Develop “light warning” disclosure of security risk
- Restrict use of personal email account by care teams
- Remove patient’s name, initials, or medical record number from email subject line

Agenda

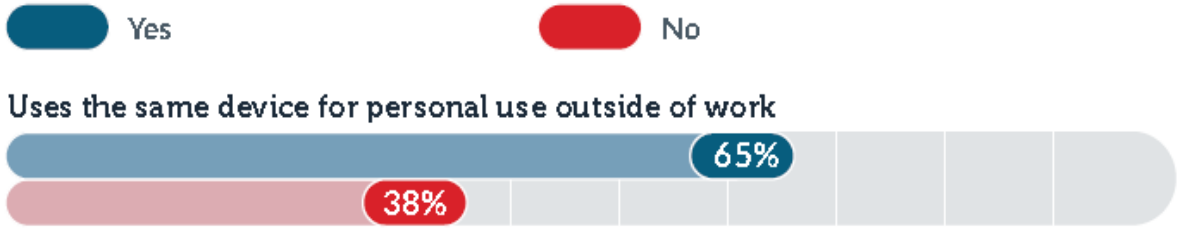
- Enforcement Landscape
- Selected HIPAA Rules
- Communication Technologies
  - Portals
  - Email
  - BYOD
  - Texting
  - Mobile Apps
  - IoT
- Evaluating and Contracting with Vendors
- Review of Compliance Strategies

Do you allow staff to bring their own devices to work and use them to communicate with patients?

Most Health Care Professionals Use the Same Device for Work and Personal Use

Portals | Email | **BYOD** | Texting | Apps | IoT

Do you use the same device for personal use outside of work?



Source: Scrypt.

BYOD

Portals | Email | **BYOD** | Texting | Apps | IoT

Advantages

- High adoption rate
- Flexibility of approach
- Productivity
- Cost advantages
- Native technologies

Disadvantages/Risk Factors

- No remote disabling or wiping w/o app
- Inadequate protection of device
- Improper device disposal or re-use
- Forcing password or authentication
- Patient-initiated communications
- Monitoring/Auditing

Practice Tips:

- Evaluate and document the risks versus benefits
- Create a detailed policy – include right of employer to access
- Workforce training; sanctions policy
- Consider mobile device management tool
- Offboarding process

BYOD Use Case: Sharing an ePHI Photograph

- Richard is a 79 year old man who undergoes surgery to remove a kidney stone. After the surgery, his doctor, Dr. Rose takes a picture of the kidney stone on his personal phone. He configured security settings so that access is protected by a combination of passcode, fingerprint recognition and timed screen locking features. He emails a copy of the picture to his work email, intending to upload the photo in Richard's chart.
- While discussing the surgery with Richard's daughter later that day, he sends her a text, of the kidney stone photo, using standard SMS. The text message is not encrypted in transit and at rest in the cloud. The cloud service that backs up his storage will delete the photo from his cloud account if Dr. Rose remembers to delete the photo from his device.

BYOD Use Case: Issues and Considerations

Issues

- Native security features
- Emailing/texting the photo
- Encryption
- Deleting the photo
- Security awareness
- Loss of phone
- Access of the phone

Considerations

- Risk analysis needs to address rapid shifts in technology and security landscape
- If solution is not easy to use, professionals may revert to unsecured text or email
- Pressure test P&Ps across broad spectrum of clinical service lines in multiple care settings
- Ability to monitor and enforce BYOD

Agenda

- Enforcement Landscape
- Selected HIPAA Rules
- Communication Technologies
  - Portals
  - Email
  - BYOD
  - Texting
  - Mobile Apps
  - IoT
- Evaluating and Contracting with Vendors
- Review of Compliance Strategies

Which messaging platform applications do you use for work purposes? (check all that apply)

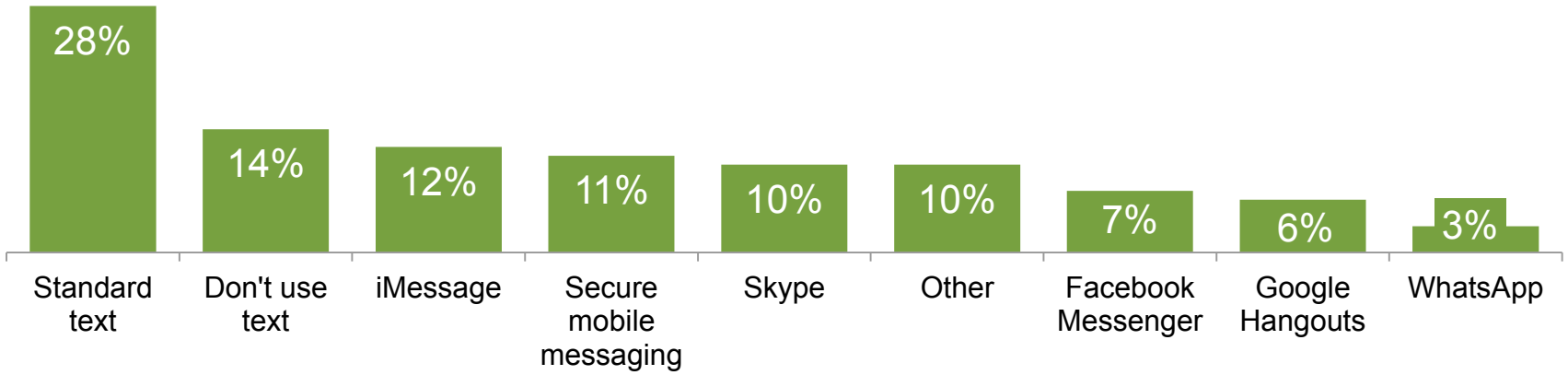
- ❑ Standard text
- ❑ Never use text
- ❑ iMessage
- ❑ HIPAA-secure messaging app
- ❑ Skype
- ❑ Other
- ❑ Facebook Messenger
- ❑ Google Hangouts
- ❑ WhatsApp

Texting

Portals | Email | BYOD | **Texting** | Apps | IoT

Texting is commonplace in many organizations. Drafting an official text policy is an essential step in a HIPAA compliance program.

Which of the following messages services or applications have you used for work purposes?



Source: Scrypt.

Texting

Portals | Email | BYOD | **Texting** | Apps | IoT

Advantages

- Increase patient engagement
- Quicker response time than email
- Adoption
- Single device
- Access control
- Cyberthreats difficult to execute with SMS

Disadvantages/Risk Factors

- Secure messaging apps require web-accessible device or smartphone
- Added HIPAA compliance responsibilities for tech vendor and downstream BA
- Traditional SMS is not encrypted
- Cyberthreats difficult to detect

Practice Tips:

- Patient consent needed
- Address retention period and when to document a patient's chart
- Evaluate use of public messaging platforms
- Properly wipe mobile devices after discontinued use for work

Texting

Portals | Email | BYOD | **Texting** | Apps | IoT

ONC FAQ: Can you use texting to communicate health information, even if it is to another provider or professional?

Answer: It depends. Text messages are generally not secure because they lack encryption, and the sender does not know with certainty that the message is received by the intended recipient. Also, the telecommunication vendor/wireless carrier may store the text messages. However, your organization may approve texting after performing a risk analysis or implementing a third-party messaging solution that incorporates measures to establish a secure communication platform that will allow texting on approved devices.

https://www.healthit.gov/providers-professionals/faqs/can-you-use-texting-communicate-health-information-even-if-it-another-p

Texting: ONC Sees Its Value

Beacon Communities – SMS Text Pilots

- Reasons for selecting SMS texting
  - Cell phones, and their use for texting, are widespread among the traditionally underserved and hard-to-reach groups
  - A growing body of evidence supports the feasibility of using text messaging for health promotion, behavior change (smoking cessation), chronic disease management, medication adherence, prenatal care, weight loss and physical activity
  - Program participants report positive user satisfaction and self-reported behavior change
  - Program managers found increased enrollment rates when potential participants were able to "opt-in" immediately to the SMS program. They also identified higher rates of patient "activation" among participants that enrolled via text message or by confirming their participation via text message after their participating enrolling in the program using an online portal

Texting: ONC Sees Its Value

- By contrast, program staff found significantly lower rates of enrollment and subsequent program participation when potential enrollees provided their contact information and consent in writing to a third party, who entered enrollment information afterwards
- Reasons given:
  - the time lag between initial sign-up and confirmation of participation in the program;
  - the provision of incorrect or incomplete contact information by potential participants
  - the lack of direct personal participation in the enrollment process

Practice Tip: HIPAA Security Rule

- **Address the encryption/integrity implementation specifications for electronic transmissions**
- **Consider whether encrypted texting is reasonable and appropriate for a given context**
- **Document equivalent, alternative measures. "Light warning" of security risk. Opt-in? Opt-out?**

Texting: Not Just a HIPAA Concern

Overlapping jurisdiction with FCC when HIPAA covered entities initiate text messages to patients

- Even if the content is for a permissible HIPAA purpose, TCPA restricts the use of automatic telephone dialing system to dial a cellular telephone number without a recipient's **prior express consent**
- Regarding informational, noncommercial messages, individuals "who knowingly release their phone numbers have in effect given their invitation or permission to be called at the number which they have given, absent instructions to the contrary"
- *Hudson v. Sharp Healthcare (9th Circuit)*
  - The call need not be made "for the exact purpose for which the number was provided" as long as the call bears some relation to the product or service for which the number was provided

A patient goes into an ambulatory surgical center for elective hip surgery. During admission, he gives his cell phone number, and the cell phone number of his daughter, who he has named as his personal representative. Can the ASC send post-operative discharge instructions via text message to the patient's daughter?

Informational Health Care Calls

- Ultimately, the facts surrounding an individual's release of his or her cell phone number will determine the scope of consent
- In the specific context of informational health care calls, the FCC states that the knowing release by a patient of a phone number to a health care provider constitutes prior express consent when the calls are:
  - Subject to HIPAA
  - Made by a HIPAA covered entity or business associate acting on its behalf
  - Closely related to the purpose for which the telephone number was originally provided

Post-surgical discharge instructions

Considerations When Developing a Policy for Texting

- Workforce training on the appropriate use of work-related texting
  - The American Health Information Management Association suggests that texting services should be included in compliance training programs
- Maintain device/media controls for mobile devices of professionals that create, receive, or maintain text messages with ePHI
- Delineate permitted use cases. For each use case:
  - Define minimum necessary identifiers
  - Place limits on the type of ePHI that can be shared via text message
  - Document the risk-based analysis
  - Develop policies and procedures for encouraging use of more secure alternative
- Consider the role of a patient advisory counsel

Considerations When Developing a Policy for Texting With Patients

- Procedures for verifying phone numbers and authenticating identity
- Decide on form and scope of consent
  - When can consent be inferred by recipient's text replies?
  - Always require opt-in?
- Disclosures to patient
  - Unsecured message
  - Opt out at any time
  - Determine policies and procedures for gathering electronic or written signatures for consents
- Use of autodialers

Considerations When Developing a Policy for Texting Between Professionals

- Consider use of a HIPAA-secured platform designed to support care team collaboration
- Secure devices in ways that allow native features (camera) to be used, but without storing photos on the device
- Device/media controls
- When text messaging should be documented in the patient's chart
  - Oral consent is permissible, but more difficult to prove
- Prohibit texting medical orders

Agenda

- Enforcement Landscape
- Selected HIPAA Rules
- Communication Technologies
  - Portals
  - Email
  - BYOD
  - Texting
  - Mobile Apps
  - IoT
- Evaluating and Contracting with Vendors
- Review of Compliance Strategies

Mobile Apps

Portals | Email | BYOD | Texting | **Apps** | IoT

Advantages

- Purpose-built, user-centered design
- Optimized native device technologies
- Through cloud-service platforms, access to state-of-art security and performance
- Cost efficiencies
- Pilot to scale

Disadvantages/Risk Factors

- Lack of standard approach to implementing security safeguards
- 1st, 2nd and n-tier business associates
- Monitoring a large vendor portfolio
- Role of app service platforms
- Convergence of HIPAA and non-HIPAA related functions in app

Practice Tips:

- Risk analysis requires an understanding of the service environment
- Develop app-specific policies/procedures within context of a risk framework and governance organization
- Negotiate master service level and BAAs with platform vendors

Mobile Apps: Use Case

You are the Chief Privacy Officer of a health system that operates in an area with high diabetes rates and poverty level, and expects to be at risk for 70% of its patient population by the end of 2017.

The CMIO is interested in a start up called RxMedPlan. RxMedPlan offers a PC-based workflow that allows health care professionals to create personalized medication schedules for patients. The solution also includes a patient mobile app and a physician app. The mobile app includes reminders,

RxMedPlan aims to release new features, including secure texting, an on-call pharmacist support center and integration with voice recognition and machine learning technologies to improve user experience and improve self-care. The health system's major vendors have promised similar mobile apps, but will not commit to a release date

The CMIO wants to move forward with a pilot of RxMedPlan and asks you for HIPAA-related guidance. What do you do?

Mobile Apps

When is an app developer a business associate?

General Advice and Health Information	Autonomous Coaching	Information Exchange	Communicating with Covered Entity or Business Associate	Medical-Grade Data
Published Content	Care Bot	Personalized Medication Schedule	On Call Pharmacist Support	Vitals Tracking

Texting

OCR FAQ:

When is a mobile app developer a business associate?

Answer: Developers are likely to be acting as business associates when "creating or offering the app on behalf of a covered entity (or one of the covered entity's contractors). The likelihood of it being a BA is high when the app involves access to ePHI in order to perform a HIPAA covered function on the covered entity's behalf

source: https://hipaaqsportal.hhs.gov/community-library/accounts/92/925889/OCR-health-app-developer-scenarios-2-2016.pdf

Mobile Apps

A covered entity (or business associate) should understand the environment or solution offered by a particular vendor so that the covered entity can appropriately conduct its own risk analysis and establish risk management policies, as well as enter into appropriate service levels and BAAs.

Tech Stack				
UI	Touchscreen	Voice recognition	Web-access	Video
Device	Mobile	Voice	PC	App platform
APIs	Security	3rd party integration		
Computing	Algorithmic processing	Human assistance	Machine learning	
Data	Public	Clinical	IoT	Self-report
Cloud Infrastructure	Storage and processing capacity, safeguards, service levels, managed services			

Agenda

- Enforcement Landscape
- Selected HIPAA Rules
- Communication Technologies
  - Portals
  - Email
  - BYOD
  - Texting
  - Mobile Apps
  - IoT
- Evaluating and Contracting with Vendors
- Review of Compliance Strategies

IoT

Portals | Email | BYOD | Texting | Apps | **IoT**

Advantages

- Medical grade devices
- Subject to FDA cybersecurity standards

Disadvantages/Risk Factors

- Device inventory and management
- Firmware patches/updates
- Undetected vulnerabilities
- Transmission security
- Wiping of ePHI between deployments

Practice Tips:

- Satisfactory assurances of compliance with FDA Quality System regulation
- Clearly define device management procedures

Agenda

- Enforcement Landscape
- Selected HIPAA Rules
- Communication Technologies
  - Portals
  - Email
  - BYOD
  - Texting
  - Mobile Apps
  - IoT
- Evaluating and Contracting with Vendors
- Review of Compliance Strategies

How do you evaluate your vendors?

A. **IT conducts a security assessment**
B. **We ask for a copy of their recent security assessment**
C. **We visit their data center**
D. **We enter into a BAA**
E. **We do all of the above for major IT vendors**
F. **We only do D regardless of the vendor-type**

Covered Entity Obligations: Evaluate

Evaluate | Document | Contract | Monitor

- Evaluate the nature of the arrangement
  - What type of PHI, if any, is being shared? By who?
  - How does this impact the risk profile?
- Offshore
  - HIPAA permits but may be other regulatory limitations
  - If ePHI is maintained in a country where there are documented increased attempts at hacking or other malware attacks, such risks should be considered, and entities must implement reasonable and appropriate technical safeguards to address such threats
- Does the vendor provide a mechanism for conducting and completing mandatory HIPAA audits?
- Willingness to share security specs
- Years of experience in health care security

Covered Entity Obligations: Evaluate (cont'd)

Evaluate | Document | Contract | Monitor

- Create a due diligence checklist
  - Ability to generate reports on access controls
  - Backup process
  - Redundant servers/server security
  - Authentication
  - Who is going to control access and authentication?
  - Retention periods customizable to match organization's policy
  - Access controls: Can you add/remove/modify users directly through current Active Directory (AD) infrastructure?
  - Is vendor using software that is certified as compliant by ONC?
  - Vendor solution has been audited and certified by 3rd party. Vendor has training and procedures in place to properly handle PHI
- If it is a large enough contract, send your security officer to do a site inspection

Covered Entity Obligations: Document

Evaluate | **Document** | Contract | Monitor

Document the evaluation

Would you be able to easily pull a list of all your business associates?

Covered Entity Obligations: Contract Term Checklist

Evaluate | Document | **Contract** | Monitor

- Business Associate Agreement - It's not always a one size fits all
  - Confirm who owns the data
  - Confirm what can be done with the data
  - Indemnification
  - Liability Caps
  - Mitigation of Breaches
  - Cyber liability coverage?
  - Reporting timeframes reasonable within the organization
  - Is the BAA consistent with the master agreement?
  - Tracking BAA (BA relationships often originate or are managed by business units versus legal or compliance departments)

Covered Entity Obligations: Service Level Agreements

Evaluate | Document | **Contract** | Monitor

- Service Level Agreements are commonly used to address more specific business expectations between the business associate and its customer, which also may be relevant to HIPAA compliance. For example, SLAs can include provisions that address such HIPAA concerns as:
  - System availability and reliability
  - Back-up and data recovery (e.g., as necessary to be able to respond to a ransomware attack or other emergency situation)
  - Manner in which data will be returned to the customer after service use termination

Covered Entity Obligations: Monitor

Evaluate	Document	Contract	**Monitor**

- Include Vendors in the annual risk assessment
- Require vendors to provide copies of their own risk assessments
- Monitor and audit their activity
- Follow-up on any reported incident that could be deemed a Security Incident or breach

Agenda

- Enforcement Landscape
- Selected HIPAA Rules
- Communication Technologies
  - Portals
  - Email
  - BYOD
  - Texting
  - Mobile Apps
  - IoT
- Evaluating and Contracting with Vendors
- Review of Compliance Strategies

Review of Compliance Strategies

- Evaluate each technology uniquely, analyzing the advantages, disadvantages and risks
  - Maintain documentation of the evaluations
- Developing HIPAA policies and procedures for digital technologies does not happen in a vacuum
  - Develop, adopt and annually review policies and procedures
  - Include all forms of technology
- Train staff on the use of these technologies to communicate with patients and among professionals, and reinforce such training

Review and Compliance Strategies

- Thoughtfully evaluate each potential vendor
- Ensure vendor evaluations are documented
- Engage in a contracting process that is reflective of the uniqueness of that vendor and the ePHI at risk
  - Impose necessary requirements on vendors to provide adequate protections
- Monitor and audit covered entities activities as they relate to use of communication technologies
- Monitor and audit BAs
- Maintain easily retrievable list of all business associates
- Address any risks and, if there is a decision not to address the risk, document why
- Consider cyber liability insurance

Questions?

Jill DeGraff Thorpe, JD
Partner, Manatt Health
jdegraff@manatt.com
202.585.6656

Helen Pfister, JD
Partner, Manatt Health
hpfister@manatt.com
212.830.7277

Randi Seigel, JD
Counsel, Manatt Health
rseigel@manatt.com
212.790.4567