HIPAA Compliance Issues and Mobile App Design

Washington, D.C.
April 22, 2015

Presenter:
Shannon Hartsfield Salimone, Holland & Knight LLP,
Tallahassee and Jacksonville, Florida

Holland & Knight

Agenda

- Whether HIPAA applies
- HIPAA overview
- Common scenarios and unintended consequences
- General HIPAA compliance obligations
- HIPAA documentation
- Architecting around HIPAA

Holland & Knight

Wait a Minute, Why Would HIPAA Possibly Apply?

- HIPAA does not apply to all health information.
- Covered entities:
  - Health plans
  - Health care clearinghouses
  - Health care providers – but not all of them
- Business associates and subcontractors

HIPAA in a Nutshell – Basic Definitions

- HIPAA defines "health care provider" broadly as any "person or organization who furnishes, bills, or is paid for health care in the normal course of business."
- "Health care" means care, services, or supplies, related to the health of the individual.
  - Apps that involve calorie counting, exercise tracking, medication reminders, etc.

HIPAA Overview

- Health care providers are "covered entities" only if they transmit PHI electronically in connection with a standard transaction.
- PHI – Protected health information – relates to past, present or future health or condition, or payment for care.
- Standard transactions include claims, payment and remittance advice, coordination of benefits, plan enrollment, etc.

PHI Examples

- Geographic subdivisions smaller than a state
- All elements of dates (except year)
- Email addresses
- Medical record numbers
- Device identifiers and serial numbers
- URLs, IP addresses
- Any other unique identifying number, characteristic or code.

If they "relate to" individuals' health, condition, or payment for their care.

HIPAA Overview – Health Care Providers

- Covered health care providers
  - Doctors, hospitals, pharmacies, etc., but only if they engage in electronic standard transactions
  - Or a third party does so on their behalf (e.g., billing company)
- Non-covered health care providers (potentially)
  - Some student clinics
  - Device manufacturers
  - Cash only medical spas and diet centers

HITECH Act

- Passed on February 17, 2009
- Extends many HIPAA provisions to business associates
- Business associates can be subject to penalties
- Individuals must be notified if the privacy or security of their protected health information is breached
- Requires revised business associate agreements (BAAs)
- Rules still to come: Expanded accounting for disclosures from electronic health records

Business Associates and Subcontractors

- Create, receive, maintain, or transmit PHI
- On behalf of the covered entity or organized health care arrangement perform, or assist in the performance of:
  - A function or activity regulated by HIPAA (data analysis, practice management, etc.)
  - Includes BA subcontractors

Holland & Knight

Business Associates

- A mobile app developer, software company, cloud storage company, etc.
- HIOs, e-prescribing gateways, and others that provide data transmission that need access to PHI on a routine basis
- Includes personal health record (PHR) vendors when acting “on behalf of”

Holland & Knight

Subcontractors

- A person to whom a business associate delegates a function, activity, or service, other than a workforce member.
- Even if you don't serve health care providers, health plans, or health care clearinghouses, you may still be subject to HIPAA as a subcontractor.

Do individuals have to comply with HIPAA?

§1320d–6. Wrongful disclosure of individually identifiable health information

(a) Offense

A person who knowingly and in violation of this part-

(1) uses or causes to be used a unique health identifier;

(2) obtains individually identifiable health information relating to an individual; or

(3) discloses individually identifiable health information to another person,

shall be punished as provided in subsection (b) of this section. For purposes of the previous sentence, a person (including an employee or other individual) shall be considered to have obtained or disclosed individually identifiable health information in violation of this part if the information is maintained by a covered entity (as defined in the HIPAA privacy regulation described in section 1320d–9(b)(3) of this title) and the individual obtained or disclosed such information without authorization.

Common Scenarios

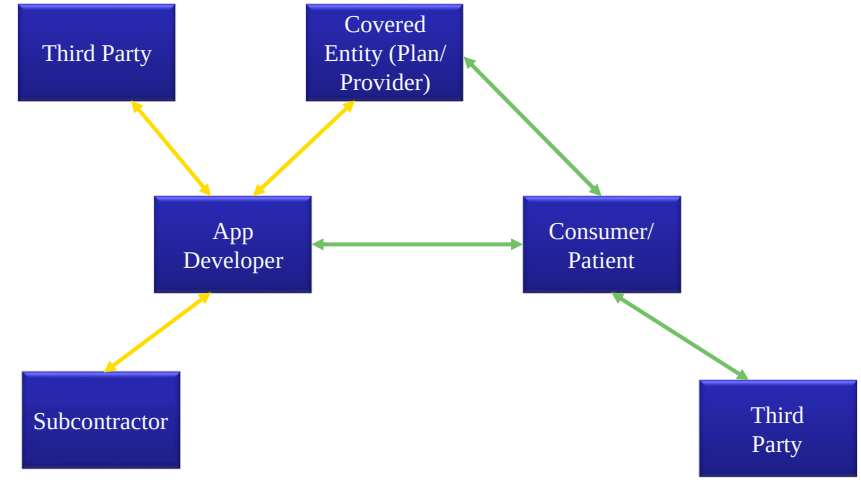
- Consumer-directed apps
- Apps with Doctor Portal Component
- Apps with Data Feed to Doctors
- Apps with an Insurance Industry Component
- Cloud storage

Holland & Knight

HIPAA Privacy Rule

- Governs the use and disclosure of PHI.
- HIPAA requires authorizations for most uses and disclosures other than treatment, payment, and health care operations.

Holland & Knight



Holland & Knight

Overview: HIPAA Privacy Standards

TPO	May use and disclose PHI for treatment, payment and operations without patient authorization
Minimum Necessary	May not use, request or disclose anything more than the minimum amount of information necessary (e.g., everyone in organization may not need access to PHI)
Incidental Disclosures	Minimize inadvertent disclosures and limit access to those with a need to know
Safeguards	Put in place physical safeguards and policies and procedures to limit unauthorized access to PHI

Holland & Knight

HIPAA Patient Rights

- Access
- Amendment
- Accounting

Holland & Knight

Designated Record Set

Image: Microsoft Corporation

- Designated record sets are records that contain PHI and that are used to make decisions about individuals

Holland & Knight

HIPAA Security Rule

- HIPAA Security Rule requires covered entities to ensure the confidentiality, integrity and availability of electronic PHI.
- Must protect against reasonably anticipated threats or hazards.

Holland & Knight

18

Security Standards

Administrative Safeguards

Involves implementing administrative functions to satisfy the security standards

Technical Safeguards

Involves the automated processes used to protect data and control access to data

Physical Safeguards

Involves protections for electronic systems and equipment

Holland & Knight

HIPAA Breach Rule

- "Breach" is the "unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information . . ."
- A number of things are not "breaches" under HITECH

Holland & Knight

Breach Risk Assessment Factors

- Nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
- The unauthorized person who used the PHI or to whom the disclosure was made;
- Whether the PHI was actually acquired or viewed; and
- The extent to which the risk to the PHI has been mitigated.

Holland & Knight

Breaches and Enforcement

- Focus is on risk to the data, rather than harm to the individual
- Enforcement activity is driven by breach reports
- Don't forget state law

If HIPAA Does Apply, What Formal Documents are Required?

- Notice of Privacy Practices?
- Policies and procedures – privacy, security, disaster recovery, etc.
- Risk analysis and mitigation plan
- Designation of Security Official (and Privacy Official?)
- Business associate agreements with covered entities
- Business associate subcontractor agreements
- Training documentation

Unintended Consequences

Holland & Knight

Sale of PHI

- Warning – Use extreme caution if PHI and remuneration are flowing in opposite directions. Does an exception apply?
- It is a crime to sell identifiable health information for commercial advantage

Holland & Knight

Sales of PHI

- Are services or products offered in exchange for access to PHI? Is PHI being sold?
  - Remuneration might involve in-kind benefits, rather than cash

Use of PHI

- Targeted advertisements
- Use of PHI beyond treatment, payment, or health care operations may require patient authorizations
- HIPAA authorizations must conform to very specific requirements, and possibly additional state laws.
  - Expiration dates or events
  - Plain language
  - Disclaimers

Disclosure of PHI

- Disclosure of PHI beyond treatment, payment, or health care operations may also require patient authorization.
- State law may require written patient authorization even for disclosures that HIPAA allows (e.g., Florida).

Other considerations for mobile apps

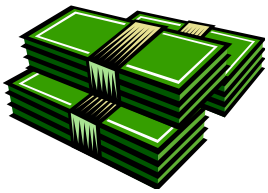
- Patient brokering/anti-kickback statutes/fee splitting
  - It is a crime knowingly and willfully to offer, pay, solicit or receive any remuneration to induce or recommend the referral of any item or service for which payment may be made under a state or federal health care program.
  - Remuneration means the transfer of anything of value.
  - AKS may be implicated even if only one purpose of the arrangement is to induce referrals.
- OIG has blessed the provisions of electronic kiosks in physician offices if they have *no independent value* to the physicians.
- Free hardware, software or services may implicate AKS if they save a physician time or money or otherwise provides value.

Other Considerations for Mobile Apps

- Inadvertently leaking PHI
- Sharing PHI inappropriately with analytics companies, advertisers, or hosted solutions
- Failure to encrypt data traffic to and from the app
- Failure to adequately or accurately disclose to users how their information will be collected and shared
- Using PHI for advertising or marketing
- Touting that the app is "HIPAA compliant"

Holland & Knight

CMP Penalty Ranges:



- Per violation (74 Fed. Reg. 56127):
- Did Not Know: $100 - $50,000
- Reasonable Cause: $1,000 - $50,000
- Willful Neglect – Corrected: $10,000 -$50,000
- Willful Neglect – Not Corrected: $50,000

  Multiple violations of an identical provision in a calendar year: Up to $1,500,000

Holland & Knight

Criminal Penalties

- Knowing violation: Up to $50,000 or 1 year of imprisonment or both
- False pretenses: Up to $100,000/5 years imprisonment
- Intent to sell, transfer, or use health information for commercial advantage, personal gain or malicious harm: Up to $250,000/10 years imprisonment

Architecting around HIPAA

- Software only?
- Conduit?
- Avoiding covered entities?
- Patient authorization?
- De-identification?

Software Only?

- Consider avoiding PHI altogether
- Providing software, by itself, doesn't make you a business associate
- Do you need access to PHI for troubleshooting, though?

Holland & Knight

Conduit Exception?

- Limited to transmission services (whether digital or hard copy) including any temporary storage of transmitted PHI incident to such transmission.
- Entities that act as mere conduits for the transport of PHI but do not access the PHI other than on a random or infrequent basis are not business associates.
- If a data transmission organization does not require access to PHI on a routine basis, they would be a conduit and not a business associate.
- Entities that manage the exchange of PHI through a network including providing record locator services and performing various oversight and governance functions for electronic health information exchange have more than random access to PHI and would be a business associate.
- Even though an entity that transmits PHI and the entity that maintains PHI both have access to PHI, the difference is the transient versus persistent nature of that opportunity.

Holland & Knight

Avoiding Covered Entities and Business Associates?

- Are you really acting "on behalf of"?
- Are you a health care provider receiving PHI for treatment?

Patient authorizations?

- May not let you avoid the business associate designation.
- Authorization forms must meet very specific (and lengthy) requirements.

De-identification of PHI?

- Individually identifiable health information from which any and ALL identifiers of the individual, relatives, employers, or household members are removed:

Holland & Knight

De-identification Safe Harbor

- ~~(A) Names;~~
- ~~(B) Street address, town or city, county, precinct, zip code, and equivalent geo-codes (other than state);~~
- ~~(C) All elements of dates (except year) for dates directly related to an individual and all ages over 89;~~
- ~~(D) Telephone numbers;~~
- ~~(E) Fax numbers;~~
- ~~(F) Electronic mail addresses;~~
- ~~(G) Social security numbers;~~
- ~~(H) Medical record numbers;~~
- ~~(I) Health plan ID numbers;~~
- ~~(J) Account numbers;~~
- ~~(K) Certificate/license numbers~~
- ~~(L) Vehicle identifiers and serial numbers, including license plate numbers;~~
- ~~(M) Device identifiers/serial numbers;~~
- ~~(N) Web addresses (URLs);~~
- ~~(O) Internet IP addresses;~~
- ~~(P) Biometric identifiers, incl. finger and voice prints;~~
- ~~(Q) Full face photographic images and any comparable images; and~~
- ~~(R) Any other unique identifying number, characteristic, or code.~~

Holland & Knight

Excerpts from Google Privacy Policy (emphasis added red)

"Device information

We collect device-specific information (such as your hardware model, operating system version, unique device identifiers, and mobile network information including phone number). Google may associate your device identifiers or phone number with your Google Account.

* * *

Unique application numbers

Certain services include a unique application number. This number and information about your installation (for example, the operating system type and application version number) may be sent to Google when you install or uninstall that service or when that service periodically contacts our servers, such as for automatic updates.

Local storage

We may collect and store information (including personal information) locally on your device using mechanisms such as browser web storage (including HTML 5) and application data caches.

* * *

Holland & Knight

Excerpts from Google Privacy Policy (emphasis added red) (cont.)

How we use information we collect

We use the information we collect from all of our services to provide, maintain, protect and improve them, to develop new ones, and to protect Google and our users. We also use this information to offer you tailored content – like giving you more relevant search results and ads."

We may combine personal information from one service with information, including personal information, from other Google services – for example to make it easier to share things with people you know.

Holland & Knight

HIPAA compliance steps

- Understand HIPAA and state law regarding data privacy
- Determine whether and how HIPAA applies
- Conduct an accurate and thorough risk analysis
- Implement a risk mitigation plan
- Address business associate and subcontractor agreements
- Develop policies and procedures
- Develop privacy notices
- Train workforce
- Audit and monitor compliance

Holland & Knight

Considerations for Patient Portals and Mobile Applications

- Defining the entity
- Analyzing the flow of PHI
- Determining whether any uses or disclosures of PHI require patient authorizations
- Implementing adequate data security

Holland & Knight

Compliance Resources http://www.hhs.gov/ocr/privacy/index.html

- Covered entity decision tree: http://www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/HIPAAGenInfo/AreYouaCoveredEntity.html
- Frequently asked questions: http://www.hhs.gov/ocr/privacy/hipaa/faq/index.html
- Audit protocols: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html
- Guidance: http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/index.html; http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html
- Enforcement: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/index.html
- BAA provisions: http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html
- Regulation text: http://www.hhs.gov/ocr/privacy/hipaa/administrative/combined/index.html
- Contact information: http://www.hhs.gov/ocr/office/about/rgn-hqaddresses.html

Holland & Knight

44

Other resources

- HealthIT.gov
- http://www.nist.gov/itl/csd/safeguarding-health-information-building-assurance-through-hipaa-security-2014.cfm
- www.himss.org

Holland & Knight

45

Questions?

Holland & Knight

Shannon Hartsfield Salimone

Shannon Hartsfield Salimone is the regulatory and litigation leader of the firm's Healthcare & Life Sciences Team. She practices in the area of health law, advising clients on state and federal healthcare regulatory matters, including corporate and regulatory compliance, data privacy, licensure, prescription drug distribution and pharmaceutical pedigree requirements and telemedicine. Ms. Salimone's clients include assisted living facilities, health plans, medical technology companies, continuing care retirement communities, nursing homes, hospitals and large clinics, pharmaceutical distributors, tissue banks, pharmacies, and medical and benefit management companies, among other members of the healthcare industry.

Shannon Hartsfield Salimone
Partner

TAL: 850.425.5642
JAX: 904.798.7331

shannon.salimone@hklaw.com
Tallahassee, Florida

Practice

- Health Law
- Data Privacy
- Compliance

Education

- Florida State University College of Law, J.D.
- Florida State University, B.A., English and Communication

Bar Admission

- Florida

Holland & Knight