Cleveland Clinic

Business Associates: Do you have Written Assurances in all the Right Places?

The Twenty Sixth National HIPAA Summit
March 30, 2017

Yvonne Wolters, CHPC
Privacy Official
Cleveland Clinic Health System

Who is a Business Associate?

- In general, a "business associate" (BA) is a person/entity (other than a member of the Covered Entity's workforce) who performs certain functions or activities that involve the use or disclosure of protected health information (PHI) on behalf of, or provides service to, a covered entity (CE).
- Business associate by definition
- A subcontractor of a BA may also be a BA
- A CE may be a BA of another CE

Reference HHS.gov: https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/

Understanding Business Associates

- Functions/activities or services provided:
  - Only those regulated by the HIPAA Rules and that are being performed for or on behalf of CE, which includes:
    - Payment or health care operations activities; and
    - Other functions or activities regulated by the Administrative Simplification Rules
  - Specific functions or activities and services performed are described in more detail at 45 CFR 164.103
- BA may not use the CE's PHI for its own independent uses or purposes, other than proper management and administration of the BA

Considerations

- Disclosure of CE's PHI to BA of another CE
- Incidental disclosures
- CE's participating in organized health care arrangement (OHCA)
- An organization who's merely a conduit (e.g., private couriers, electronic equivalents)
- Disclosure to a researcher under certain circumstances (i.e., authorization or waiver)
- Telehealth and medical device companies

Look in the Mirror

Who your BA's are may not be so obvious!

- Affiliate
- Subsidiary
- Spin-off
- Separate legal entity
- Partnership
- Doing business as (d.b.a.)
- Single covered entity
- Affiliated covered entity
- Accountable care organization
- Network participant

Jennifer Steinkamp, *Mike Kelley*, 2007, video installation. Main Campus.

Office for Civil Rights Enforcement

Raleigh Orthopaedic Clinic: No BA Contract

2016: Failed to obtain written satisfactory assurances w/BA. Impermissibly disclosed PHI to third party vendor w/out BA contract. $750K Settlement

SEMC: PHI on an Internet App

2016: Failed to renew or modify existing BA contracts. Impermissibly disclosed PHI to vendor w/out BA contact. $400K Settlement

Oregon Health & Science University

2016: > 3,000 individuals' PHI on a cloud-based server w/out a BA contract. Unencrypted laptops and thumb drives w/PHI. Did not act in a timely manner to address risks identified in risk analysis. $4.8M Settlement

Advocate Health – No BA Contract or P&Ps

2016: Failed to accurately perform RA & RM. Failed to execute written satisfactory assurances w/BA. Failed to implement P&Ps. Impermissibly disclosed PHI w/out BA contract in place. $5.5M Settlement

Limited Data Set (LDS)

- LDS is PHI
- Used in research, health care operations & public health
- Recipient of LDS is not a BA, unless meet definition of BA
- Must execute Data Use Agreement
- If recipient of LDS is CE, then CE must comply with HIPAA & directly liable to OCR enforcement
- May include any of the following identifiers:
  - Town or city, State and zip code
  - Elements of dates related to health care and the individual
  - Unique identifying numbers, characteristics, or code

Reference HHS.gov: https://www.hhs.gov/hipaa/for-professionals/special-topics/research/index.html?language=es

Breaches by Business Associates

Must notify without unreasonable delay but no later than 60 days from date of discovery:

- BA must notify CE
- CE must Notify:
  - Impacted individuals; and
  - Government & media, as required (< or > 500)
  - CE's discovery date is when BA notified CE; unless agent of CE
- CE may delegate individual breach notice to the BA via BAA
  - CE ultimately responsible for compliance with the Rule

Written Satisfactory Assurances Required

- Business Associate Contract* - says BA will comply
  - Certain provisions of Privacy Rule – safeguard PHI and use and disclose PHI only as permitted or required under the Rule; ***and***
  - Security Rule – appropriately safeguard PHI it creates, receives, maintains, or transmits on behalf of the CE
  - BA obligated to execute BA contract with its BA subcontractors
- Sample BA Contract at HHS.gov
- If no PHI involved, then not a BA
  - Other contracts or agreements may be needed

*Certain elements required in the BA contract can be found at 45 CFR 164.504(e)

Once the ink is dry, then what?

- Generally, workforce has misperception that once contract signed, it's a green light to go – it's Legal!!
  - Potential risk if expect workforce to know next steps for compliance
- Goal is to protect health information
- Understand the operations; follow PHI
- Update security risk analysis
- Ensure reasonable and appropriate safeguards in place

Consider This…

- CE looking for data analysis services at a good rate and quality work.
- Contractor says they have the latest technology and experienced IT personnel. Their services also come with technical support for the life of the services provided.
- They have a subcontractor who uses special tools to de-identify patient information, if needed.
- The contractor provides documents explaining they are HIPAA compliant.
- What do you do?

Covered Entity's Obligations

CE NOT required to monitor BA's HIPAA compliance

However, CE must:

- Comply with Privacy Rule, such as:
  - Execute written assurances
  - Reasonable and appropriate safeguards
- Comply with Security Rule Administrative Safeguards
  - Risk analysis and risk management (164.308(a)(1))
  - And many more

Understanding Minimum Necessary

- Applies directly to CE's and BA's
- Only use/disclose the limited PHI needed for the intended purpose or particular function
- Applies to uses, requests and disclosures of PHI for:
  - Payment and/or health care operations
  - Access controls – role based access
- Flexible - your assessment of what is reasonably necessary
- Not intended to sacrifice quality of care!

Reference Federal Register: https://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf

Understanding Minimum Necessary

Minimum necessary standard does not apply to the following disclosures of PHI:

- Disclosures to or request by a health care provider for treatment; professional judgment does apply
- Disclosures to the individual who is the subject of the information
- Pursuant to a patient's authorization
- Required for compliance with the HIPAA Rules
- To the Department of Health & Human Services (HHS) when required for enforcement purposes
- That are required by other law; other limits and conditions may apply

Required Documentation

CE must develop and implement policies and procedures to comply w/minimum necessary:

- Routine/recurring requests and disclosures:
  - Policies and procedures or standard protocols that limit the PHI to the amount reasonably necessary
- All other requests and disclosures:
  - Develop criteria designed to limit the PHI to the amount reasonably necessary
- Omnibus Rule – BA contract must limit BA's uses/disclosures to be consistent with CE's minimum necessary policies & procedures
- Uses – access controls; role-based access

Reasonable Reliance

- Permitted (not required) to rely on the judgment of the requesting party that the information requested *IS* the minimum necessary:
  - A public official or agency
  - Another covered entity
  - A workforce member of a BA
  - A researcher with appropriate documentation from an Institutional Review Board or Privacy Board
- Reasonable reliance is CE's discretion

Workforce Training

Ensure workforce members are aware

- Where to obtain guidance w/in the entity for determining BA relationships (CE's and BA's)
- Implement required policies and procedures, for example:
  - Reasonable and appropriate safeguards
  - Minimum necessary
  - Incident reporting
  - Accounting of disclosures

Consider Other Privacy Requirements

For example:

- State Law
- Confidentiality of Alcohol & Drug Abuse Patient Records Regulation (42 CFR Part 2)
- Meaningful Use
- The Joint Commission
- Centers for Medicare/Medicaid Services (CMS)

Amy Stein, *Return*, 2005, digital c-print. Main Campus.
Courtesy Amy Stein

Questions?

Presenter Information

Yvonne Wolters, CHPC
CCHS Privacy Official
216.444.5192 or woltery@ccf.org

Resources/References

- Sample Business Associate Agreement and required elements in the BA contract.
  - https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html
- HHS Minimum Necessary Guidance
  - https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/minimum-necessary-requirement/index.html
- Office for Civil Rights Enforcement
  - https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/

Cleveland Clinic

Every life deserves world class care.