Advanced Resident Privacy: Considerations in the Age of Smart Devices and Other Electronic Traps

Maureen Molony

Dan Balk

von Briesen & Roper, s.c.

Milwaukee | Madison | Fox Valley - Green Bay | Waukesha County

www.vonbriesen.com

Overview

- Federal Privacy Rights
- State Privacy Rights
- Application to SNF and AL

Federal Law:

HIPAA & HITECH

HIPAA 101:

PRIVACY STANDARDS

HIPAA Privacy Objectives

- Give individuals more control over their health information
- Set boundaries on use and disclosure of health information
- Establish appropriate safeguards for all people who participate or are involved with the provision of health care to ensure they honor individuals' right to privacy of their health information
- Hold violators accountable through civil and criminal penalties

Who Must Comply: Covered Entities

Health Plans

- Individual and group plans that provide or pay for the cost of medical care
- Health insurance issuers, commercial insurance policies, HMOs, PPOs, group health plans, government programs (Medicare, Medicaid)

Health Care Clearinghouses

- Entities that process or facilitate the processing of health information
- Billing services, repricing companies

Health Care Providers

- Provider of health services that transmits health information in electronic form to carry out financial or administrative activities
- Physicians, group practices, hospitals, SNFs, pharmacies, labs

Hybrid Entities

- Single legal entity with both covered and non-covered functions
- Covered functions must comply
- Counties, municipalities, school districts, EMS departments

Who Must Comply: Business Associates

Individuals or entities that:

- Perform (or assist in performing) a function or service
- For or on behalf of a covered entity or other business associate
- That involves the creation, receipt, maintenance, or transmittal of health information

Individually Identifiable Health Information

Information, including demographic data, that relates to:

- the individual's past, present, or future physical or mental health or condition;
- the provision of health care to the individual; or
- the past, present, or future payment for the provision of health care to the individual;

and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual

What Makes Information Identifiable?

1. Name
2. Address (geographic subdivisions smaller than a state)
3. Email address
4. Dates (except years)
   - Birth Date
   - Admission/Discharge Dates
5. Telephone numbers
6. Fax numbers
7. Social Security Number
8. Medical record number
9. Health plan beneficiary number
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers
13. Device identifiers and serial numbers
14. URLs
15. IP addresses
16. Biometric identifiers, including finger and voice prints
17. Full face photographic images and any comparable images
18. Any other unique identifying number, characteristic, or code (not the unique code assigned by the investigator to code the data)

All 18 elements must be removed for data to be de-identified.

Privacy Standards:

USE AND DISCLOSURE OF PHI

Use and Disclosure

Privacy Rule limits circumstances under which an individual's health information may be used or disclosed

- Use: the sharing, employment, application, utilization, examination, or analysis of PHI within the entity that maintains the PHI
- Disclosure: the release, transfer, provision of access to, or divulging in any manner, PHI outside the entity holding the PHI

Use and Disclosure

- General Rule: An entity may not use or disclose PHI except as permitted or required by the Privacy Rule
- An entity may use and/or disclose PHI pursuant to a valid authorization
- Treatment, payment, and health care operations (TPO)

Individual Rights

- Accounting of disclosures
- Request to amend PHI
- Access to PHI (including right to electronic copy)
- Restrict disclosures to health plans for out-of-pocket items/services
- Notice of Privacy Practices

Compliance Considerations

- Review privacy policies and procedures
  - Appropriate use/disclosure restrictions and processes
  - Are you ready to address individual requests?
  - What response timeframes have you agreed to?
  - Audit
- Document!
- Workforce training

HIPAA 101:

BREACHES

What is a Breach?

- The acquisition, access, use, or disclosure of PHI in a manner not permitted by the Privacy Rule which compromises the security or privacy of PHI
- Breach is *presumed* unless CE or BA demonstrates there is a low probability that the PHI has been compromised based on a risk assessment

Four Factors: Low Probability of Compromise

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

What is Not a Reportable Breach?

- *Unintentional use* by workforce member in good faith, within scope of authority, and without further impermissible disclosures
- *Inadvertent disclosure* by person authorized to access PHI to another person authorized to access PHI at the same CE or BA without further impermissible disclosures
- Unauthorized recipient *not reasonably able to retain PHI*

Notification Timing Remains

- Affected individuals: Notice without unreasonable delay and in no case later than 60 days following breach
  - 60 calendar days is an outer limit
  - OCR may determine that notification should have been reported sooner
  - Content requirements remain
- HHS via annual breach log: breach affects < 500 people
- HHS without unreasonable delay and within 60 days: breach affects > 500 people
- Media: breach affects > 500 people

Compliance Considerations

- Tabletop exercises – be prepared for quick response
- Pay attention to the risks from technology
  - Personal and mobile devices, encryption
- Review breach investigation and response policies and procedures
  - Document your breach risk assessment process
- Insurance coverage

Wisconsin Privacy Laws

RESIDENT RIGHTS

Recent Focus

- In 2016, DQA released new guidance on use of electronic devices and resident recording

Resident Rights

- Under Chapter 50, residents of SNFs and CBRFs have a right to:
  - Private and unrestricted communications
  - Physical and emotional privacy in treatment, living arrangements and careing for personal needs

Resident Rights - SNF

- Under federal law:
  - Right to personal privacy and confidentiality of personal and medical records. Includes:
    - Accommodations, medical treatment, personal care, visits, meetings of family and resident groups.
    - Private oral, written, and electronic communication
  - Freedom from abuse, including mental abuse
    - S&C Letter described unauthorized recording of residents as mental abuse

Resident Rights - CBRF

- Explicit right not to be recorded, filmed or photographed without informed, written consent by the resident or resident's legal representative.

Potential Issues

HANDHELD/SMART DEVICES

Recording – Facility Initiated

- Means by which a facility, *or others acting on the facility's behalf*, record residents:
  - Security cameras
  - Installation of smart devices
  - Posting by staff and volunteers

Recording by Third Parties

- Other ways residents are recorded
  - Other residents using handheld devices
  - Other residents using smart devices
  - The resident's visitors including family, friends, etc.
  - Other resident's visitors

Avoid issues and address violations

PREVENTION AND RESPONSE

Prevention

- Determine resident desires in advance
- Training staff early and often
- Drafting and enforcing policies
- Restricting the use of devices in common areas
- Informing visitors on arrival
- Actively monitoring the facility

Response

- Protect residents first (if possible, delete posting)
- Discipline offending staff, reeducate others
- For third parties, consider how to prevent further incidents (constrain visitation rights?)
- Revise procedures to prevent further incidents

Response

- Determine reporting obligations
  - OCR
  - DHS
  - OCQ
  - Law enforcement?
  - Etc.

ADDITIONAL CONSIDERATIONS

Types of Devices

- Smart home (Alexa, google assistant, portal)
- Passive vs. active recording
- Ability to “drop in”
- Cell phones
- Security cameras

Installation by Resident

- Where installed?
- Where used?
- Can facility limit installation or use?
- Policy and Acknowledgement Form

Installation by Family

- Where installed?
- Resident’s competency?
- Does family have legal authority to consent for resident?

Installation by Facility

- Where installed?
- What types of devices?
- Staff use of cell phones

Questions?

Daniel J. Balk
414-287-1583
dbalk@vonbriesen.com

Maureen A. Molony
608-661-3995
mmolony@vonbriesen.com