# MANAGING PHI ACCESS AND PERMISSIONS – STEPS TO REDUCE YOUR RISKS

HCCA BOSTON REGIONAL CONFERENCE
SEPTEMBER 2017

## Today's Program

2

- Today's program examines HIPAA-regulated entities' risks related to their management of access and permissions for PHI, from three different angles:
  - A review of relevant OCR activity of *non-technical* issues
    - Access considerations beyond technical security safeguards or managing information systems
  - The view from a Chief Compliance Officer
    - Access to Social Security and insurance numbers
  - A deep dive into a specific OCR Resolution Agreement that demonstrates the importance of watchfully managing workforce access through technical and other means
    - Terminating user access and monitoring system activity to detect suspicious access

## Technical Security Noise Crowding Out Other Areas?

3

- Managing Access and Use Permissions goes well-beyond technical security controls, it includes a host of considerations including administrative and physical safeguards for paper and electronic records
  - Focus on these areas can reduce your risk immediately
- Failure to perform an adequate security risk assessment is the most prevalent issue in the Resolution Agreement, cyber-threats are the most prominent news item
- But it is important not to lose sight of the broader issues for managing access and use permissions
  - You cannot control everything, but there are basic areas of focus, beyond assessing security risks and cyber-threats, that can improve your risk profile

## Gatekeeper Role

4

**The Gatekeeper role is to ensure authorized access to PHI, which includes stopping unauthorized access to PHI**

**All authorized access and PHI use permissions need to be planned, follow written policies, and cover the universe of PHI in your control**

## Tracking OCR Resolution Agreements

5

- Office for Civil Rights (OCR) has a variety of notices and tools designed to help organizations remain HIPAA compliant, including, a running list of Resolution Agreements:
  - www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/
- The Resolution Agreements are designed to be parables to industry on what OCR thinks is important in HIPAA compliance
- Tracking and reviewing these should be part of routine compliance processes

## Issues You Need To Review (Right Now)

6

- **Check to be sure you have a Bring-Your-Own-Device Policy**
  - While the rules do not expressly state that you must have a BYOD policy, OCR has made it known that they will ask for a copy of your policy
- **Include Paper Records In Your Self-assessments**
  - There have been multiple Resolution Agreement penalties for failure to shred or properly safeguard paper records
  - You need a policy for when paper is allowed "offsite"
  - You need a competent shredding system

## Business Associate Agreements Are Not Optional

7

- **Be sure you have an *up-to-date* business associate arrangement in place for *every one* of your business associate relations**
  - April 2016: $750,000 penalty. Ortho group did not obtain a BAA before releasing x-ray films of 17,300 patients to a company that transfers images to electronic media, in exchange for harvesting the silver from the x-ray films
  - September 2016, $400,000 penalty. Outdated BAA between a hospital and system. BAA was dated 2005, but not updated for 2010 or 2013 changes (until 2014)
  - April 2017, $31,000 penalty. Provider failed to have a BAA with its **paper records storage company**

## Media Access and Communications

8

- **Check to be sure you have a written policies for filming patients, using their information in your promotional materials, and media contact**
  - April 2016: $2.2m penalty. Hospital allowed the TV show "NY Med" to film patients, and disclosed PHI about patients
  - February 2016: $25,000 penalty. Physical therapy provider posted patient testimonials (photos and identifying information) online without patient authorizations
  - May 2017: $2.4 million penalty. Hospital called police on person presenting with false identity, all fine and HIPAA compliant up to that point. But hospital issued a press release about the incident, **including** the person's name

# Filming, Social Media, Promotions

9

- Ensure that media pressure, or self-imposed pressures to tell your story, do not interfere with patents' privacy rights
- Work to control what is within your control: set reasonable policies for workforce and visitors
  - You should remove inappropriate posts on *your own* social media pages
  - But you are *not required* to stop all friends and family from their personal Facebook use or using their own phones
    - Suggestion: Do not tackle visitors to get their phone
    - Suggestion: Try de-escalation techniques when visitor policies are not being followed

# UMass Memorial Breach

**Police detail alleged theft of IDs by former UMass Memorial employee**

By Brian Lee TELEGRAM & GAZETTE STAFF
Posted Nov 11, 2014 at 6:00 AM
Updated Nov 11, 2014 at 10:17 AM

WEBSTER — A former employee of the University of Massachusetts Memorial Medical Center in Worcester and her daughter and her daughter's boyfriend allegedly stole the identities of approximately 22 people to buy cellphones and utility services via the Internet, investigators said.

## Bottom Line

- By removing or limiting access to Social Security numbers and insurance numbers, health care entities can reduce the risk of identity theft for patients and the organization
  - **Remove** SSN and insurance numbers from applications where not needed
  - Where needed, **limit** users access to this information as required for job functions
- By improving **audit** capabilities, may also be able to respond more precisely to a data breach

## Is All PHI and PII Created Equal?

- HIPAA applies equally to all 18 PHI identifiers
- State Regulations focus on:
  - Social Security numbers
  - Driver's license or state ID
  - Financial account number/debit or credit card number
- All of the above must be protected from inappropriate use and disclosure

# Market Value of Data

| Hacker service | Price |
|---|---|
| Social Security number (sold as part of 'Fullz' dossier) | $30 |
| Date of birth | $11 |
| Health insurance credentials | $20 |
| Visa or MasterCard credentials | $4 |
| American Express credentials | $7 |
| Discover credit credentials | $8 |
| Credit card with magnetic stripe or chip data | $12 |
| Bank account number (balance of $70,000 to $150,000) | $300 or less |
| Full identity 'Kitz' | $1,200 to $1,300 |

Bankrate.com, July 27, 2015

# Why Focus on SSN and Insurance Numbers?

- Value, particularly with other information available in health records
- Insurance number is sometimes a SSN
  - Medicare will replace SSN-based Health Insurance Claim Number with Medicare Beneficiary Identifier between April 2018 and April 2019
- Often used to authenticate a person
  - When you call your bank, what do they ask for?
- Can be used to open accounts for credit and services
- Often broadly available within health care applications
  - But are they always needed?

## Valid Uses

- Insurance claim submission
- Identifying patient insurance
- Identifying patients
- Government registries
- Research

## Remove SSN and Insurance Numbers

- Many health care applications or modules include this information, but don't need it
  - Part of their original build
  - Not necessary for all health care operations; clinical vs. financial or HR systems
  - Can link to other applications or modules using other identifiers, such as MRN
  - In these cases, turn off feeds and eliminate the information
    - Significant IT involvement, use change control, have a back out plan
  - To respond to a past data breach that is discovered in the future, create a forensic file
    - Which patients had valid SSN or insurance number
    - Date removed

## Where Data Needed, Limit Access

- Determine with managers what roles require access to SSN or insurance to perform their job duties
- Determine the roles available within the application and whether they can limit display of SSN or insurance number
  - May not be as precise as desired, resulting in access due to need for unrelated data or functions
  - Assess access to, and need to include within, reports and printed forms, such as face sheets
- For SSN, preference for masking all 9 digits
  - State regulations typically permit access to last 4
  - Last 4 often used as an authenticator by banks, etc.
  - Roles where needed typically require all 9 or none

## Audit

- Breaches will happen
- Evaluate audit log for roles with access to SSN or insurance numbers
  - Access to application
  - Access to a patient
  - Access to a screen
  - Access to a field

# Sample SSN Audit Results

| Accessed Application | Accessed Patient | Accessed Screen | Accessed Field |
|---|---|---|---|
| 1,797,284 | 166,697 | 355 | 30 |
| | | | |

- Consider data breach notification implications
  - If the nature of the breach is the theft of SSN, without an audit trail that goes to the field level, health care entities may be significantly over-notifying patients and regulators

**RESOLUTION AGREEMENT**

I. Recitals

1. **Parties**. The Parties to this Resolution Agreement (Agreement) are

A. The United States Department of Health and Human Services, Office for Civil Rights ("HHS"), which enforces the Federal standards that govern the privacy of individually identifiable health information (45 C.F.R. Part 160 and Subparts A and E of Part 164, the "Privacy Rule"), the Federal standards that govern the security of electronic individually identifiable health information (45 C.F.R. Part 160 and Subparts A and C of Part 164, the "Security Rule"), and the Federal standards for notification in the case of breach of unsecured protected health information (45 C.F.R. Part 160 and Subparts A and D of 45 C.F.R. Part 164, the "Breach Notification Rule"). HHS has the authority to conduct compliance reviews and investigations of complaints alleging violations of the Privacy, Security, and Breach Notification Rules (the "HIPAA Rules") by covered entities and business associates, and covered entities and business associates must cooperate with HHS compliance reviews and investigations. *See* 45 C.F.R. §§ 160.306(c), 160.308, and 160.310(b).

B. South Broward Hospital District d/b/a Memorial Healthcare System ("MHS") is a covered entity, as defined at 45 C.F.R. § 160.103, and therefore is required to comply with the HIPAA Rules. MHS is a non-profit corporation and an independent special tax district under the laws of the State of Florida which operates six hospitals, a nursing home, and a variety of ancillary health care facilities throughout the South Florida area. MHS is the third largest public health care system in the nation.[1]

HHS and MHS shall together be referred to herein as the "Parties."

2. **Factual Background and Covered Conduct.**

On April 12, 2012, MHS submitted a breach report to HHS indicating that two MHS employees inappropriately accessed patient information, including names, dates of birth, and social security numbers. On July 11, 2012, MHS submitted an additional addendum breach report to notify HHS that during its internal investigation, it discovered additional impermissible access by 12 users at affiliated physician offices, potentially affecting another 105,646 individuals.[2] Some of these instances led to federal charges relating to selling protected health information (PHI) and filing fraudulent tax returns.

HHS's investigation indicated that the following conduct occurred ("Covered Conduct"):

A. MHS impermissibly disclosed the PHI of 80,000 individuals in violation of the Privacy

[1] http://www.mhs.net/aboutus/
[2] MHS reported a total of 111,650 affected individuals to OCR, but notified 115,143 individuals by letter. According to MHS's response on November 2, 2015, the latter number is accurate as the number affected.

RA/CAP 12-141825 page 1 of 15

## The Incident

- Several separate incidents
- Reported in April 2012 (MHS employees)
- Continued investigation
- Reported in July 2012 (Affiliated physicians)
- Corrective action
  - Millions of dollars spent
  - Administrative, technical and physical safeguards
  - New personnel and structure for privacy and security

## The OCR Investigation

- Took 5 years
- 3 different investigators
- 6 rounds of requests
- Months and sometimes years between requests
- Types of requests

## The Negotiation

- Investigator on maternity leave
- Worked with deputy regional manager without HHS AGC
- Opening settlement amount
- Other resolution agreements
- Protracted negotiations
- Final negotiations by covered entity, not counsel

## Corrective Action

24

- Assessor
- Approval of plan by OCR
- New policies and procedures
- Training of employees
- Technical enhancements
- Sliding timeline

# Wrap Up

25

- Questions?

- Contact Information:
  - Jen Cox, (860) 727-4004, jcox@coxlawoffices.com
  - Rick King, (774) 442-9450, richard.king@umassmemorial.org
  - Lynn Sessions, (713) 646-1352 lsessions@bakerlaw.com