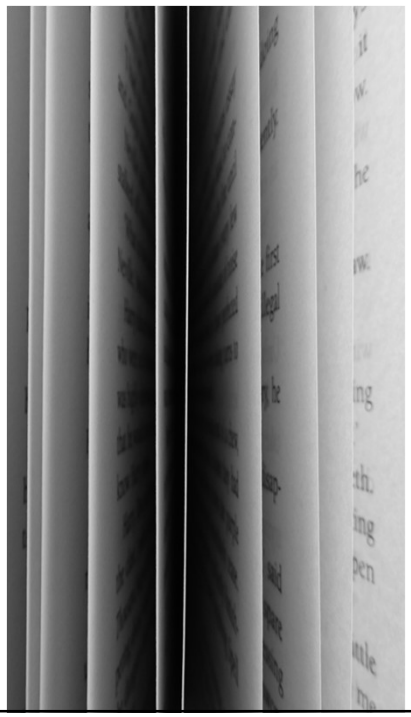

Privacy Breach Response

Healthcare Enforcement Compliance Conference

November 4, 2019
Washington, DC

Blaine Kerr, CISA, CHPC
Chief Privacy Officer
Jackson Health System

Greg Kerr, MJ, CHPC, CHC
Chief Privacy Officer
Ensemble Healthcare Partners

1

Session Objectives

- A discussion of the importance of being proactive about data security and how information security is a dynamic process that must assess risks to e-PHI on an ongoing basis
- Strategic insights to navigate interaction with the media such that protected health information is not disclosed in an egregious way
- Methods to assess when a Business Associate Agreement is necessary and the obligations of the Business Associate throughout the life cycle of PHI

2

2

The Before…

The best time to minimize your risks

Having a game plan is a necessity…not a luxury

3

3

Before a Data Breach

- Complete an annual privacy and security risk assessment
- Create a plan to assess privacy and security incidents
    - Breach circumstances
    - Nature of the unauthorized disclosure
    - Type of data involved
    - Applicable regulations and regulators
    - Potential level of harm to affected individuals

4

4

Before a Data Breach (continued)

- Develop a breach response
  - Internal stakeholders
  - Vendors (forensic review, notification mailing and call center services, identity and credit monitoring
- Update policies and procedures
  - Changing technologies
  - Updated state or federal reporting requirements

5

5

During…

Tensions are sky high

Kneejerk reactions can be costly

Gather the facts

Provide a proportionate response

6

6

During Discovery of a Data Breach

- Complete a forensic investigation
  - Determine the nature and severity of the incident
  - Document findings – may help you with a regulatory investigation or class-action litigation
- Determine if there is a notifiable breach
  - Affected individuals, OCR, State Regulator Requirements
  - Timelines and residency of affected individuals
  - Media and Substitute Notice
  - Remediation (policies and systems)
  - Credit monitoring and identity recovery services

7

7

After…

Effects are not always immediate

Look for additional steps needed

Continue demonstrating commitment to safety of data and stakeholders

8

8

After a Data Breach

- Monitor the status of affected individuals
  - Number who reported being a victim
  - Utilization of recovery services offered
- Review and position reputational promotion and recovery
- Assess cyber liability risks and potential benefits of insurance
  - Your needs against a policy's offerings
  - Utilization of recovery services offered

9

9

Navigation with the Media

FOR IMMEDIATE RELEASE
May 10, 2017
Contact: HHS Press Office
202-690-6343
media@hhs.gov

Texas health system settles potential HIPAA disclosure violations

*"Senior management should have known that **disclosing a patient's name on the title of a press release** was a clear HIPAA Privacy violation that would induce a swift OCR response,"* said OCR Director Roger Severino. *"This case reminds us that organizations can readily cooperate with law enforcement without violating HIPAA, but that they must nevertheless continue to protect patient privacy when making statements to the public and elsewhere."*

- Memorial Hermann Health System (MHHS) is a not-for-profit health system located in Southeast Texas, comprised of 16 hospitals and specialty services in the Greater Houston area.

10

10

Navigation with the Media

- **MHHS agreed to pay $2.4 million** to the U.S. Department of Health and Human Services (HHS) and adopt a comprehensive corrective action plan to settle potential violations of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule.
- In September 2015, a patient at one of MHHS's clinics presented an allegedly fraudulent identification card to office staff. The staff immediately alerted appropriate authorities of the incident, and the patient was arrested. This disclosure of PHI to law enforcement was permitted under the HIPAA Rules.
- **MHHS subsequently published a press release concerning the incident in which MHHS senior management approved the impermissible disclosure of the patient's PHI by adding the patient's name in the title of the press release.** In addition, MHHS failed to timely document the sanctioning of its workforce members for impermissibly disclosing the patient's information.

11

11

Navigation with the Media

FOR IMMEDIATE RELEASE
November 26, 2018
Contact: HHS Press Office
202-690-6343
media@hhs.gov

Allergy practice pays $125,000 to settle doctor's disclosure of patient information to a reporter

"OCR's investigation found that the doctor's discussion with the reporter demonstrated a reckless disregard for the patient's privacy rights and that the disclosure occurred after the doctor was instructed by Allergy Associates' Privacy Officer to either not respond to the media or respond with "no comment." Additionally, OCR's investigation revealed that Allergy Associates failed to take any disciplinary action against the doctor or take any corrective action following the impermissible disclosure to the media."

12

12

Navigation with the Media

1. Allergy Associates is a health care practice that specializes in treating individuals with allergies, and is comprised of three doctors at four locations across Connecticut
2. A patient of Allergy Associates contacted a local television station to speak about a dispute that had occurred between the patient and an Allergy Associates' doctor. The reporter subsequently contacted the doctor for comment and the doctor impermissibly disclosed the patient's PHI to the reporter.
3. OCR's investigation found that the doctor's discussion with the reporter demonstrated a reckless disregard for the patient's privacy rights and that the disclosure occurred after the doctor was instructed by Allergy Associates' Privacy Officer to either not respond to the media or respond with "no comment."
4. Furthermore, Allergy Associates failed to take any disciplinary action against the doctor or take any corrective action following the impermissible disclosure to the media.

13

13

Navigation with Social Media

FOR IMMEDIATE RELEASE
October 2, 2019
Contact: HHS Press Office
202-690-6343
media@hhs.gov

Dental Practice Pays $10,000 to Settle Social Media Disclosures of Patients' Protected Health Information

"Social media is not the place for providers to discuss a patient's care," said OCR Director, Roger Severino. *"Doctors and dentists must think carefully about patient privacy before responding to online reviews."*

14

14

Navigation with Social Media

1. OCR received a complaint from an Elite Dental Associates' patient alleging that Elite had responded to a social media review by disclosing the patient's last name and details of the patient's health condition.
2. OCR's investigation found that Elite had impermissibly disclosed the protected health information (PHI) of multiple patients in response to patient reviews on the Elite Yelp review page
3. Additionally, Elite did not have a policy and procedure regarding disclosures of PHI to ensure that its social media interactions protect the PHI of its patients or a Notice of Privacy Practices that complied with the HIPAA Privacy Rule.
4. OCR accepted a substantially reduced settlement amount in consideration of Elite's size, financial circumstances, and cooperation with OCR's investigation

15

15

When a BAA is necessary and the Obligation of BAAs

- Develop the approval process and include the appropriate subject matter experts
  - Privacy
  - Departmental Leadership
  - Legal
  - Procurement/Purchasing
- Maintain updated repository
  - Name, contact information, service line provided
  - Timing for reporting

16

16

Business Associate Agreements

FOR IMMEDIATE RELEASE
December 4, 2018
Contact: HHS Press Office
202-690-6343
media@hhs.gov

Florida contractor physicians' group shares protected health information with unknown vendor without a business associate agreement

"OCR's investigation revealed that Advanced Care Hospitalists PL ("ACH") never entered into a business associate agreement with the individual providing medical billing services to ACH, as required by HIPAA and failed to adopt any policy requiring business associate agreements until April 2014."

17

17

Business Associate Agreements

1. ACH engaged the services of an individual that represented himself to be a representative of a Florida-based company named Doctor's First Choice Billings, Inc. (First Choice). The individual provided medical billing services to ACH using First Choice's name and website, but allegedly without any knowledge or permission of First Choice's owner.

2. A local hospital notified ACH that PHI was viewable on the First Choice website.

3. OCR's investigation revealed that ACH never entered into a business associate agreement with the individual providing medical billing services to ACH, had not conducted a risk analysis or implemented security measures or any other written HIPAA policies or procedures before 2014

18

18

Business Associate Agreements

FOR IMMEDIATE RELEASE
December 11, 2018
Contact: HHS Press Office
202-690-6343
media@hhs.gov

Colorado hospital failed to terminate former employee's access to electronic protected health information

"OCR's investigation revealed that Pagosa Springs Medical Center (PSMC") impermissibly disclosed the ePHI of 557 individuals to its former employee and to the web-based scheduling calendar vendor without a HIPAA required business associate agreement in place."

19

19

Business Associate Agreements

1. The settlement resolved a complaint alleging that a former PSMC employee continued to have remote access to PSMC's web-based scheduling calendar, which contained patients' ePHI, after separation of employment.

2. *"It's common sense that former employees should immediately lose access to PHI upon their separation from employment,"* said OCR Director Roger Severino. *"This case underscores the need for covered entities to always be aware of who has access to their ePHI and who doesn't."*

3. Covered entities that do not have or follow procedures to terminate information access privileges upon employee separation risk a HIPAA enforcement action. Covered entities must also evaluate relationships with vendors to ensure that BAAs are in place with all business associates before disclosing PHI.

20

20

Questions?

21

21