BREAKOUT SESSION

HIPAA PRIVACY AND SECURITY ENFORCEMENT

PBI

MARCH 13, 2019

Charles I. Artz, Esq. • John Mayernick, IV, Esq.

I. PERSONAL DATA BREACH LITIGATION HIPAA SECURITY IMPLICATIONS

- Dittman v. UPMC/University of Pittsburgh Medical Center, 196 A.3d 1036 (Pa. 2018)
  - Trial Court and PA Superior Court dismissed complaint
  - PA Supreme Court reversed dismissals
  - Negligence claim was allowed for data breach

Seven UPMC employees individually, and on behalf of a class action, sued UPMC for negligence and damages as a result of a data breach.

II. HIPAA Privacy Violation - $4.348M Judgment Stolen Unencrypted Laptop Lost USB Drives

Fourth largest recovery ever secured by OCR.

- Office for Civil Rights v. University of Texas MD Anderson Cancer Center, No. C-17-854 (CR5111 2018)
  - All mobile devices containing PHI/ePHI should be encrypted/password protected.
  - Never allow employees to remove from the practice premises ePHI on a mobile device without proper encryption/password protection.
  - Repeatedly train providers/staff on compliance requirements.
  - Lost or stolen mobile device containing ePHI may constitute "disclosure" requiring the filing of Breach Notification to OCR.
  - Investigate violations promptly; impose sanctions/suspension or termination for cause.

III. Physician Convicted By Federal Jury Of Illegally Sharing Patient Medical Files

- U.S. v. Luthra, No. 15-CR-30032-MGM (D. Mass. 2018)
  - Sentenced to 1 year probation on September 19, 2018

Physician was convicted by a federal jury for violating the Wrongful Disclosure of Individually Identifiable Health Information criminal provision under the HIPAA Privacy statute, 42 U.S.C. §1320d-6, because she asked a pharmaceutical company's sales representative to help her medical assistant with securing prior authorizations for expensive medications marketed by the pharmaceutical company without signing a Business Associate Agreement.

IV. Provider Held Liable For Business Associate Data Breach -- $418,000 Fine State Attorney General Enforcement

Practice violated the HIPAA Privacy and Security regulations as a result of a data breach caused by the practice's *business associate*.

- *In re* Virtua Medical Group
  - New Jersey Attorney General's office (as opposed to the federal OCR) initiated the case.
  - Third party vendor failed to implement adequate security measures.
  - Provider was held fully responsible for conduct that was clearly the fault of the business associate because it was the provider's data that was breached and the provider was ultimately responsible for that data.

V. Medical Practice HIPAA Privacy Violation Unauthorized PHI Disclosure -- $125,000 Fine

- *In re* Allergy Associates
  - Medical group practice, through one of its physicians, impermissibly disclosed patient's PHI to unauthorized third party.
  - Medical group practice failed to apply appropriate sanctions against physician.

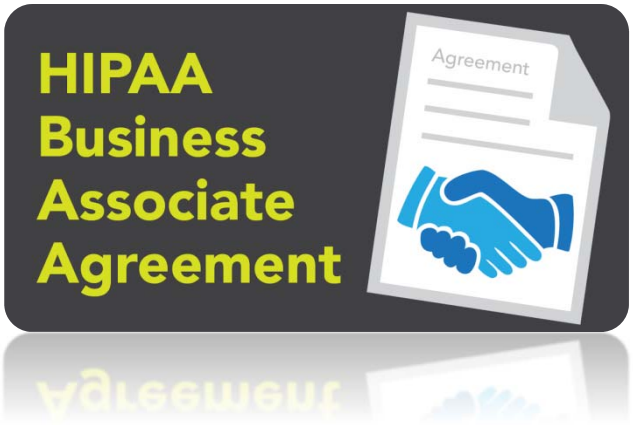
- Patient alleged she was refused access to allergy medical practice because of the use of her service animal.
- Patient contacted local TV station to complain.
- TV reporter contacted physician for comment.
- Physician impermissibly disclosed patient's PHI.

VI. HIPAA Privacy/Security Violation – Failure To Terminate Access After Employment Ends Another Business Associate Agreement Violation

- *In re* Pagosa Springs Medical Center
  - $111,400 Fine and Corrective Action Plan Imposed

The Provider:

- Failed to deactivate former employee's user name, password and access to PHI following termination.
- Impermissibly disclosed PHI of at least 557 patients to business associate without obtaining satisfactory assurances in the form of a written BAA.



VII. HIPAA Security Violation Spear Phishing Cyberattack $16 Million Fine

- *In re* Anthem, Inc.

Compliance Points:

- ✓ Routinely conduct "enterprise-wide" risk analysis.
- ✓ Make sure sufficient procedures are in place to regularly review information system activity.
- ✓ Promptly identify and respond to suspected or known security incidents.
- ✓ Implement minimum access to controls to prevent cyber-attackers from accessing sensitive ePHI.
- ✓ Train all staff about "spear Phishing emails."

OCR found that Anthem failed to implement appropriate measurers for detecting hackers who gained access to their system to harvest passwords and steal people's private information.

VIII. No Private Right of Action To Enforce HIPAA Regulations

- Coley v. George W. Hill Prison,
  2018 WL 5814673
  (E.D. Pa. 2018)

- Jackson v. Mercy Behavioral Health,
  2015 WL 401645
  (W.D. Pa. 2015)

IX. Breach Of Confidentiality Tort Liability

- Lee v. Park,
  720 Fed. Appx. 663 (3rd Cir. 2017)

  - Patient sued his physician for negligence *per se*, ordinary negligence and breach of confidentiality.
  - Federal court dismissed the case prior to trial.
  - Patient appealed
  - U.S. Court of Appeals upheld the dismissal of the negligence *per se* claim, but reversed the dismissal on the ordinary negligence and breach of confidentiality claims.

At no point did the patient consent to the release of his PHI to his spouse.