
# HIPAA Crimes:

## *How the New Crime Wave Affects You*

May 17, 2016

# Speakers

**Michele L. Adelman**, Partner, Foley Hoag LLP

*White Collar Crime & Government Investigations Practice*

Michele brings over a decade of federal and state prosecutorial experience to her counsel of corporations and individuals in a wide range of government investigations, including healthcare fraud cases that allege violations of the Anti-Kickback Statute, False Claims Act, and the HIPAA Statute. Her practice includes internal investigations and compliance advice that often focus on issues relating to computer crimes and information privacy and security.

Michele has published an extensive number of articles and blog posts, and been a regular speaker on topics relating to healthcare fraud investigations and prosecutions.

**Colin J. Zick**, Partner, Foley Hoag LLP

*Chair, Data Privacy & Security Practice; Co-chair, Healthcare Practice*

Colin counsels clients ranging from the Fortune 1000 to start-ups on issues involving information privacy and security, including state, federal and international data privacy and security laws and government enforcement actions. He also frequently counsels technology and consumer-facing clients on issues involving information privacy and security, including the EU Privacy Shield, HIPAA and other U.S. federal and state data privacy and security laws, cloud security, cyber insurance, the Internet of Things, and data breach response.

Colin is a regular contributor to the firm's "Security, Privacy and the Law" blog found at: www.securityprivacyandthelaw.com.

# What Will This Program Cover?

- The current environment for HIPAA enforcement
- Types of HIPAA incidents and enforcement actions
- Related data security issues affecting health care providers
- How these issues implicate law enforcement and the criminal law aspects of HIPAA
- Steps you can take to avoid getting dragged into a HIPAA enforcement action

# Examples of Actions That Could Lead to HIPAA Liability

- Misdirected information
- Insider takes information
  - For personal reasons
  - For monetary/business reasons
- Hackers take information
  - For personal reasons
  - For monetary/business reasons
- Ransomware
- Invasion of System to Use Resources

# Range of HIPAA Compliance and Enforcement Actions

- Government audits of covered entities and business associates
- Letter with Suggestions for Changing Practices
- Civil Penalty
  - More and bigger civil monetary settlements
  - Compliance Agreement/Reporting
- Criminal Penalty

# HIPAA Statistics

- From April 2003 to the present, the compliance issues most investigated are:
  1. Impermissible use/disclosure of PHI
  2. Lack of safeguards of PHI
  3. Lack of patient access to their PHI
  4. Use/disclosure of more than minimum necessary PHI
  5. Lack of safeguards of electronic PHI

# HIPAA Statistics

- From April 2003 to the present, the most common type of Covered Entities subject to corrective action:
  1. Private Practices
  2. General Hospitals
  3. Outpatient Facilities
  4. Pharmacies
  5. Health Plans

# Violations of HIPAA?

- Who enforces the HIPAA rules?
- What happens if an individual violates HIPAA rules?
- What happens if a company violates HIPAA rules?

# Civil vs. Criminal Enforcement

- Civil enforcement by:
  - U.S. Department of Health and Human Services Office of Civil Rights ("OCR"); or
  - State attorneys general
- Criminal enforcement by U.S. Department of Justice ("DOJ") through local U.S. Attorney's Offices

# Civil vs. Criminal Enforcement

- Difference between civil and criminal enforcement is often dependent upon evidence of offender's "intent"
- Criminal enforcers often step in when violator sought to profit from the improper use or disclosure of PHI

# Civil Enforcement Stats

- HHS, Office of Civil Rights ("OCR"), reports as of March 31, 2016:
  - Since April 2003, OCR has received over 130,748 HIPAA complaints and has initiated over 885 compliance reviews
  - OCR has resolved 96% of those cases (125,472)
  - In over 24,477 cases, OCR required changes in privacy practices and corrective actions
  - OCR has settled 33 cases with civil monetary penalties totaling $33,689,200
  - In 10,979 cases, OCR found no violation
  - In 13,041 cases, OCR intervened early and provided technical assistance without the need for investigation

# Criminal Cases

- Employee does not need to be an officer/director to face personal liability
- Fundamental issue: whether the employee was a rogue, dishonest employee acting for himself, or conduct was on behalf of corporation
- Focus on who benefited from the crime

# Criminal Cases

- Principles of Corporate Criminal Liability
- Corporation is criminally liable for acts of employee or agent who has been given authority to act on behalf of corp.
- There will be liability if employee was authorized to act and engaged in criminal activity in course/scope of his/her duties

# The HIPAA Criminal Statute

- A person who knowingly and in violation of this part:
- Uses or causes to be used a unique health identifier;
- Obtains individually identifiable health  info relating to an individual; or
- Discloses individually identifiable health info to another person

# Tiered Civil Financial Penalties

- Lowest level – did not know (and by exercising reasonable diligence would not have known)
- Second level – result of reasonable cause and not due to willful neglect
- Third level – due to willful neglect, but violation is corrected within the required time period
- Most severe level – due to willful neglect, and violation is not corrected

FOLEY HOAG LLP

# Levels of Penalties

- Lowest level:  fined not more than $50K, imprisoned not more than 1 year, or both;
- False pretenses: fined not more than $100K, imprisoned not more than 5 years, or both;
- Intent to sell, transfer or use PHI for commercial advantage, personal gain or malicious harm: fined not more than $250K, prison not more than 10 years

# What is a “Knowing” Violation?

- Requires only knowledge that are engaging in actions that constitute the violation
- Does not require the Government to prove that offender “knew” that an action would violate a provision of HIPAA

# Specific Types of Conduct That Have Been Prosecuted Under HIPAA

- Identity theft of patients' PHI (most common)
- Snooping on patients' records (usually famous patients)
- Failure to report breaches in a timely manner
- Lack of adequate safeguards to protect PHI

# Criminal HIPAA Prosecution
# Joshua Hippler – Feb. 2015

- Hospital employee accessed PHI for personal gain
- Guilty plea to criminal HIPAA violation
- Sentenced to 18 months

# Florida Hospital Employees 2011 and 2014

- Florida Hospital Registration Representative, Dale Munroe, obtained PHI of patients who were involved in motor vehicle accidents
- Provided the information to co-conspirators who paid Munroe
- Co-conspirators used the information to solicit patients for lawyers and chiropractors

# Dale Munroe and Katrina Munroe

- Both Munroes pled guilty to criminal HIPAA charges and cooperated with the government
- Dale Munroe sentenced to one year and a day in prison
- Katrina Munroe sentenced to 2 years' probation

# Dale Munroe and Katrina Munroe

- Accessed records of over 700,000 patients between Jan. 2009 and July 2011
- Katrina Munroe, Dale's wife, also worked for Florida Hospital
- Between July and Aug. 2011 (one month), obtained PHI and caused the transfer of the PHI as part of the same scheme

# Florida Hospital – Round 2

- In May 2014, two other Florida Hospital employees illegally printed patient “face sheets” that contained PHI
- No evidence that these employees used the PHI for commercial gain
- Those employees were fired but not criminally prosecuted

# Huping Zhou – April 2010

- Research assistant at UCLA Health Systems accessed PHI of co-workers and celebrities with no legitimate reason
- There was no subsequent leak or sale of PHI
- Charged with misdemeanor crime of “knowingly” obtaining PHI

# Huping Zhou

- Conditional guilty plea to criminal HIPAA plea pending appellate review
- Appellate court upheld the conviction
- “Knowing” he was accessing health information was sufficient – did not have to “know” such access violated HIPAA
- Sentenced to 4 months

# What's Missing? Criminal Actions Against the Real Bad Guys

- No prosecutions for
  - Ransomware
  - Actions of organized, state-sponsored hackers
  - Hacktivists
- Why not?
- Will this change in the future?

# Helpful Hints in Dealing with Law Enforcement

- Just because you don't think you did anything wrong, you still must be wary when dealing with law enforcement.
  - Don't talk to law enforcement without first conferring with counsel.
  - But you cannot tell others not to talk to the government.
  - If you are going to refer a matter that you hope will be prosecuted, the facts must be as fully developed as possible and documented.

# Policies & Procedures Are Still Important When You Are a Victim

- Permissible and impermissible uses and disclosures of PHI
- Standards for security awareness, information access, and workstation use
- Physical removal and transport limitations
- Standard business associate agreement regarding PHI limitations under HIPAA

# How to Show Your Company in the Best Light? Conduct Regular Employee Training

- Training needs to be regular and ongoing
- Establish training protocols
- Document employee training sessions
- Address all limitations and conditions on removal of PHI from premises and remote access to PHI
- No access to PHI without training
- No sharing of passwords
- Measure the effectiveness of the training through self-audits and exit interviews

# Key Steps to Achieving HIPAA Compliance

- Perform regular self-audits
- Perform occasional third-party audits
- Document audit findings, act on those findings, and document all corrective actions
- Consider using unannounced site visits, penetration testing, and other tests aimed at policies, procedures, and human factors
- Consider when self-disclosure of problems is needed and/or beneficial

# Thank You!

**Michele L. Adelman**, Partner, Foley Hoag LLP
*White Collar Crime & Government Investigations Practice*
617.832.1278
madelman@foleyhoag.com

**Colin J. Zick**, Partner, Foley Hoag LLP
*Chair, Data Privacy & Security Practice; Co-chair, Healthcare Practice*
617.832.1275
czick@foleyhoag.com