LATHAM&WATKINS

Subtitle Here

OCR Investigations and Enforcement: Defense Perspective

David Tolley, Latham & Watkins

September 10, 2021

1

Roadmap

- Recent HIPAA Enforcement
  - Lessons from M.D. Anderson
  - Settlement Trends
- Investigation Process
  - Responding to OCR Requests
  - Settlement Negotiations

2

LATHAM&WATKINS

Recent HIPAA Enforcement

3

M.D. Anderson

- University of Texas M.D. Anderson Cancer Center ("M.D. Anderson")
- Arose out of three incidents in which employees lost patients' data:
  - In 2012, a faculty member's unencrypted laptop was stolen, containing electronic protected health information ("ePHI") for 29,021 individuals.
  - In 2013, two unencrypted USB thumb drives were also lost, containing ePHI for approximately 5,600 individuals.
- OCR determined that M.D. Anderson had violated two regulations by:
  - Failing to implement a mechanism to encrypt ePHI or adopt some other "reasonable and appropriate" method to limit access to ePHI (the "Encryption Rule"), 45 C.F.R. § 164.312, and
  - Violating regulations prohibiting the unpermitted disclosure of ePHI (the "Disclosure Rule"), 45 C.F.R. § 164.502(a).
- OCR imposed a civil monetary penalty ("CMP") of $4,348,000.
  - HHS assessed penalties for the CMP based on each day the violations occurred, resulting in penalties of:
    - $1,348,000 for the Encryption Rule violations,
    - $1,500,000 for the 2012 Disclosure Rule violations, and
    - $1,500,000 for the 2013 Disclosure Rule violations.

4

Fifth Circuit Decision (January 2021)

The Fifth Circuit overturned the CMP for four reasons:

1. The Encryption Rule does not require "bulletproof protection."
2. The Disclosure Rule does not penalize the passive loss of information.
3. HHS must "treat like cases alike."
4. HHS must ensure its monetary penalties are consistent with statutory caps set by Congress at 42 U.S.C. § 1320d-5.

5

OCR Settlements Trends

- "Right of Access"
  - An enforcement priority to support individuals' rights to timely access their health records and at a reasonable cost.
  - The majority of recent OCR settlements have been Right of Access matters.
- Cyberattacks
  - Numerous OCR settlements arise out of cyberattacks that compromised protected health information.
  - A December 2020 HIPAA Audits Industry Report stated that "[c]onsistent with the findings of OCR's compliance reviews and complaint investigations, these audits confirmed that small percentages of covered entities (14%) and business associates (17%)…are substantially fulfilling their regulatory responsibilities to safeguard ePHI they hold through risk analysis activities."

6

Examples of Recent Settlements

Entity	Date of Settlement	Resolution Amount	Facts	Key Issues	Takeaways
Banner Health (on behalf of Banner Health affiliated covered entities)	January 6, 2021	$200,000 monetary penalty Two (2) year Corrective Action Plan (CAP)	Banner Health is a non-profit health system based in Phoenix, Arizona. OCR received two complaints alleging violations of the HIPAA Right of Access standard. The first, received on August 17, 2018, alleged that an individual requested access to her medical records in December 2017, and did not receive the records until May 2018. The second, made January 3, 2020, alleged that the individual requested access to an electronic copy of his records in September 2019, and the records were not sent until February 2020. OCR's investigations determined that Banner Health ACE entities' failure to provide timely access to the requested medical records were potential violations of the HIPAA right of access standard.	Right of Access	Covered entities must ensure that they timely respond to request for a patient to access their medical records, or face HHS penalties.
Lifetime Healthcare Companies and its affiliates (collectively "Excellus Health Plan")	January 14, 2021	$5.1 million monetary penalty Two (2) year Corrective Action Plan (CAP)	Excellus Health Plan (EHP) is a New York health services corporation that provides health insurance coverage. On September 9, 2015, EHP filed a breach report stating that cyber-attackers had gained unauthorized access to its information technology systems. EHP reported that the breach began on or before December 23, 2013, and ended on May 11, 2015. The hackers installed malware and conducted reconnaissance activities that ultimately resulted in the impermissible disclosure of the protected health information of more than 9.3 million individuals. On June 29, 2019, HHS notified EHP that it was initiating an investigation on EHP's compliance with the Privacy, Security, and Breach Notification Rules. OCR's investigation found potential violations of the HIPAA Rules including failures to: (1) conduct an enterprise-wide risk analysis; (2) implement risk management, (3) implement information system activity review; (4) implement technical policies and procedures for electronic systems that contain protected health information; and (5) prevent unauthorized access of ePHI.	Cyberattack Privacy, Security, and Breach Notification	Covered entities must regularly conduct enterprise-wide risk analysis and implement polices and procedures to mitigate and monitor risks of breach or loss.

7

LATHAM&WATKINS

Investigation Process

8

Initiation of Investigation

There are two main ways OCR initiates an investigation:

1. **Complaint investigations**
   - A patient or employee reports potential HIPAA violations to the OCR.

2. **Breach Reports to OCR**
   - A covered entity or business associate reports a suspected breach to OCR
   - Breaches of over 500 affected individuals must be reported to HHS without unreasonable delay and in no case later than 60 days from discovery of the breach.
   - Breaches under 500 affected individuals must be reported to HHS within 60 days of the end of the calendar year in which the breach occurred.

9

Information Requests

Regardless of how an investigation is initiated, OCR must gather information to determine if any regulations were violated. The covered entity should:

1. **Gather Information**
   - OCR collects evidence through interviews, witness statements, requests for data from the entity involved, site visits, or other available, relevant documents.
   - Covered entities and outside counsel help collect the information and provide responsive documents to OCR.

2. **Cooperate with Investigation**
   - Investigations should not be adversarial.
   - Covered entities are required by law to cooperate with complaint investigations.

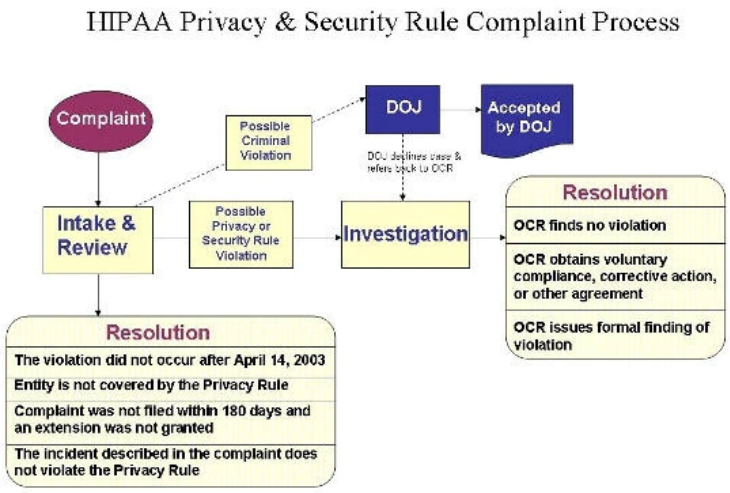
3. **Conduct Own Investigation**
   - Investigations seek to determine what happened.
   - Covered entities and outside counsel conduct their own investigation into the facts, and can present their findings to OCR.

10

Resolution

Once OCR has investigated, it can either:

1. Find no violation occurred;
2. Reach an agreement with the entity; or
3. Issue a formal finding of violation.



Penalties

OCR considers four factors when assessing CMPs:

1. The **nature and extent of the violation**
2. The **nature and extent of the harm resulting from the violation**
3. The **history of prior compliance with the administrative simplification provisions, including violations**
4. The **financial condition** of the covered entity or business associate

Penalty Amounts

Culpability	Description	Minimum Penalty* (per violation)	Maximum Penalty*	Maximum Annual Penalty*
Tier 1 ("No Knowledge")	A violation that the covered entity was unaware of and could not have realistically avoided, had a reasonable amount of care had been taken to abide by HIPAA Rules.	$119	$59,552	$1,785,651
Tier 2 ("Reasonable Cause")	A violation that the covered entity should have been aware of but could not have avoided even with a reasonable amount of care (but falling short of willful neglect).	$1,191	$59,552	$1,785,651
Tier 3 ("Willful Neglect – Corrective Action Taken Within 30 Days")	A violation suffered as a direct result of "willful neglect" of HIPAA Rules, in cases where an attempt has been made to correct the violation.	$11,904	$59,552	$1,785,651
Tier 4 ("Willful Neglect – No Timely Corrective Action Taken")	A violation of HIPAA Rules constituting willful neglect, where no attempt has been made to correct the violation.	$59,552	$1,785,651	$1,785,651

*These amounts are updated annually, as mandated by the Federal Civil Penalties Inflation Adjustment Act Improvements Act of 2015 (Inflation Adjustment Act). 45 C.F.R. § 102 (2020). The current penalties are effective January 17, 2020.

LATHAM&WATKINS

13

13

LATHAM&WATKINS

Questions?

14

14