When the Other Brother Steps Up: State Privacy Enforcement Actions

Healthcare Enforcement Compliance Conference
November 6, 2018
Washington, DC

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

Greg Kerr, MJ, CHPC, CHC
Managing Director
Ankura Consulting Group

Juan Carlos Palacio, JD, CHC
Associate Director, Health Information Privacy & Privacy Officer
Jackson Health System

1

Session Objectives

- History of state regulator enforcement with privacy violations
- Discussion of state privacy enforcement actions and trends
- Insights to navigate potential state enforcement liability
- Methods to address privacy strategies for address state breach notification requirements

2

History of State Privacy Enforcement

3

State Privacy Enforcement Actions
A Brief History

- 1990(s)
  - State Attorneys General (SAG) offices start focusing on privacy issues
  - 1991-1992 SAG bring first privacy enforcement actions using state unfair and deceptive trade acts and practices laws.
- 2000(s)
  - 2002-California first state to pass data breach notification requirements.
  - 2009-Health Information Technology for Economic and Clinical Health Act (HITECH Act) authorizes to enforce the Health Insurance Portability and Accountability Act of 1996 (HIPAA).
  - HIPAA now has breach notification requirements.

4

State Privacy Enforcement Actions
A Brief History

- 2010(s)
  - 2010-Connecticut is first state to sue a healthcare provider for failing to secure health data as required by HIPAA.
  - SAG begin to form specialized privacy units
    - Connecticut first to establish an independent privacy division.
  - 2018-All 50 states, as well as the District of Columbia, Puerto Rico, Guam, and the Virgin Islands have enacted breach notification laws.

5

And Then Came HITECH and SAG Enforcement Options

6

State Attorneys General Involvement

Section 13410(e), Signed into law on February 17, 2009

- HITECH gave SAG the authority to bring civil actions on behalf of state residents for violations of the HIPAA Privacy and Security Rules.
- The HITECH permits SAG to obtain damages on behalf of state residents or to enjoin further violations of the HIPAA Privacy and Security Rules.
- Office for Civil Rights (OCR) developed HIPAA Enforcement Training to help SAG and their staff use their new authority to enforce the HIPAA Privacy and Security Rules.
- The materials make clear that OCR expects that state authorities will take a more active role enforcing both state and federal privacy laws in the coming years.

7

Case Studies

8

2018 State Attorneys General Enforcement Actions

- January 2018-Aetna settles with New York AG for $1.15 million
- March 2018-EmblemHealth settles with New York AG for $575,000
- March 2018-VMG, a Physician Group, pays $417, 816 to the New Jersey AG and New Jersey Division of Consumer Affairs
- September 2018-UMass Memorial agreed to pay the state of Massachusetts $230,000 to settle a lawsuit brought by the Massachusetts AG
- September 2018-New York AG levies $200,000 fine on Arc of Erie County, a non-profit that provides services to people with developmental disabilities

9

Aetna Agrees to $1.15 Million Settlement with New York Attorney General

- July 2017, Aetna sent a mailing to 2,460 members in which details of HIV medications were clearly visible through the plastic windows of envelopes, inadvertently disclosing highly sensitive HIV information to individuals' house mates, friends, families, and loved ones.
- The July breach triggered a class action lawsuit which was recently settled by Aetna for $17.2 million. Aetna must now also cover the $1.15 million settlement with the New York Attorney General to resolve violations of federal and state laws.
- Attorney General Schneiderman launched an investigation following the breach of HIV information in July.
- An additional privacy breach was discovered during the course of that investigation. 163 New York Aetna members had their privacy violated by another mailing.

10

Aetna Agrees to $1.15 Million Settlement with New York Attorney General (2)

- September 2017, a similar privacy breach occurred. This time the mailing related to a research study regarding atrial fibrillation (A Fib) in which the term IMACT-AFIB was visible through the window of the envelope. Anyone who saw the envelope could have deduced the intended recipient had an A Fib diagnosis.
- Aetna provided the protected health information (PHI) of its members to outside counsel who in turn gave that information to a settlement administrator.
- The outside counsel was a business associate (BA) of Aetna and had signed a business associate agreement (BAA).
- However, the BA's subcontractor, the settlement administrator, was also a BA, yet no BAA was entered into prior to the disclosure of PHI. A further violation of HIPAA Rules.

11

Aetna Agrees to $1.15 Million Settlement with New York Attorney General (3)

- The office of the attorney general determined Aetna's two mailings violated:
  - 45 C.F.R § 164.502; 42 U.S.C. § 1320d-5 of HIPAA
  - N.Y General Business Law § 349
  - N.Y Public Health Law § 18(6)
  - N.Y Executive Law § 63(12)
- This $1.15 million settlement only resolves the privacy violations of 2,460 Aetna members in New York state.
  - The mailing was sent to around 12,000 Aetna members across the United States.

12

UMass Memorial reaches $230,000 settlement with the state of Massachusetts- September 28, 2018

- Two data breaches that exposed the PHI of more than 15,000 Massachusetts residents, according to the Massachusetts Attorney General. The complaint alleges:
  - Two UMass Memorial employees separately used patient PHI to open mobile phone and credit card accounts.
  - UMass Memorial entities violated the Consumer Protection Act, the Massachusetts Data Security Law, and HIPAA.
  - The exposed PHI included: Names, Addresses, Clinical & Health Information, Social Security numbers.
  - The settlement also includes an agreement that UMass Memorial will conduct employee background checks, train employees on proper handling of PHI, limit employee access to PHI, and promptly investigate suspected improper access.
- UMass Memorial is also required to hire an independent firm to conduct a review of its data security policies and procedures.

13

Virtua Medical Group

- March 2018-Virtua Medical Group (VMG), a physician group, pays $417,816 to the New Jersey AG and New Jersey Division of Consumer Affairs
  - VMG suffered a data breach caused by a BA when the BA inadvertently posted medical records online publicly during a File Transfer Protocol ("FTP") server upgrade.
  - In particular, the judgment asserted that VMG allegedly failed to conduct a risk analysis relating to its BA.
  - Even though the consent judgment indicated a BA caused the actual breach, VMG, the Covered Entity (CE), was nevertheless subject to an investigation that revealed alleged HIPAA violations and, subsequently, an enforcement action.

14

EmblemHealth Settles with New York AG for $575,000

March 2018:

- The New York Attorney General's office recently announced that EmblemHealth agreed through a settlement to pay $575,000 and implement a CAP to resolve alleged violations of HIPAA and New York's General Business Law § 399-ddd(2)(e). EmblemHealth used health insurance claim numbers that incorporated individuals' social security numbers on a mailing label for 81,122 people (55,664 of which resided in New York).
- The CAP requires EmblemHealth to undertake a thorough risk assessment, provide adequate workforce training, and report any security incidents to the AG's office that involve the loss or compromise of New York resident information (even if the incident would not otherwise be subject to New York breach reporting requirements).

15

2017 AG Fines for Privacy Breaches

Covered Entity	State	Amount	Individuals affected	Reason
Cottage Health System	California	$2,000,000	More than 54,000	Failure to Safeguard Personal Information
Horizon Healthcare Services Inc.,	New Jersey	$1,100,000	3.7 million	Failure to Safeguard Personal Information
SAManage USA, Inc.	Vermont	$264,000	660	Exposure of PHI on Internet
CoPilot Provider Support Services, Inc.	New York	$130,000	221,178	Late Breach Notifications
Multi-State Billing Services	Massachusetts	$100,000	2,600	Failure to Safeguard Personal Information

16

Puerto Rico Hits Insurer with Record $6.8 Million Fine for HIPAA Breach

- On February 18, 2014, Puerto Rican insurer Triple-S revealed that it will face a $6.8 million fine for violating HIPAA. According to an 8-K filing submitted to the Securities and Exchange Commission ("SEC")
- The Puerto Rico Health Insurance Administration notified Triple-S of additional sanctions for HIPAA violations to include:
  - suspension of new enrollments into one of its plans until it presents a corrective plan to avoid such HIPAA violations
  - obligation to notify affected individuals of their right to disenroll
- Triple-S was fined $6.7 million improperly handled private health records of more than 13,330 patients
- Another $100,000 fine was tacked on after the company provided vague or incomplete information during the probe

*Fine reduced to $1.5 Million on appeal

17

Liabilities & Strategies

18

Potential State Privacy Breach Enforcement Liabilities

1. Breached data may include more than PHI
2. Type of breached data (e.g. electronic, paper, verbal) may impact state privacy breach reporting requirements
3. Number of individuals impacted by the breach may trigger different state reporting responsibilities
4. Breach notification deadlines may be different than HIPAA
5. Content of breach notification letters may have varying state specific requirements
6. Multiple state agencies may need to be notified
7. Adherence to federal regulatory breach reporting requirements may satisfy state reporting requirements

19

Strategies to address state breach notification requirements

1. Quickly identify the affected individuals to include the total number and their residential addresses
2. Identify the type of PHI that was breached (e.g. electronic, paper, verbal)
3. Reference the state regulations to determine the patient breach reporting requirements to include notification time deadlines
4. Determine the state agency and regulator reporting requirements to include reporting time deadlines
5. Identify any state breach notification letter requirements
6. Be aware of state exceptions where breach notification requirements may be met if entity has federal breach notification regulatory requirements

20

Responding to a Violation or Incident Investigation

General Guidance

1. Be proactive … introduce yourself

   Reach out and establish a relationship with your local SAG office. Specifically, the unit or individual who handles breach notifications for the office.

2. Examine BAA to ensure that third party vendors bear the financial risk for failures to provide notice regarding breaches and to maintain adequate security measures to mitigate against the risk of disclosures.
3. SAG may choose to bring actions under HIPAA, but they may also choose more expansive or vague state consumer protection laws. Increasingly, a well-prepared organization will need to be fluent in both.

21

Questions?

22