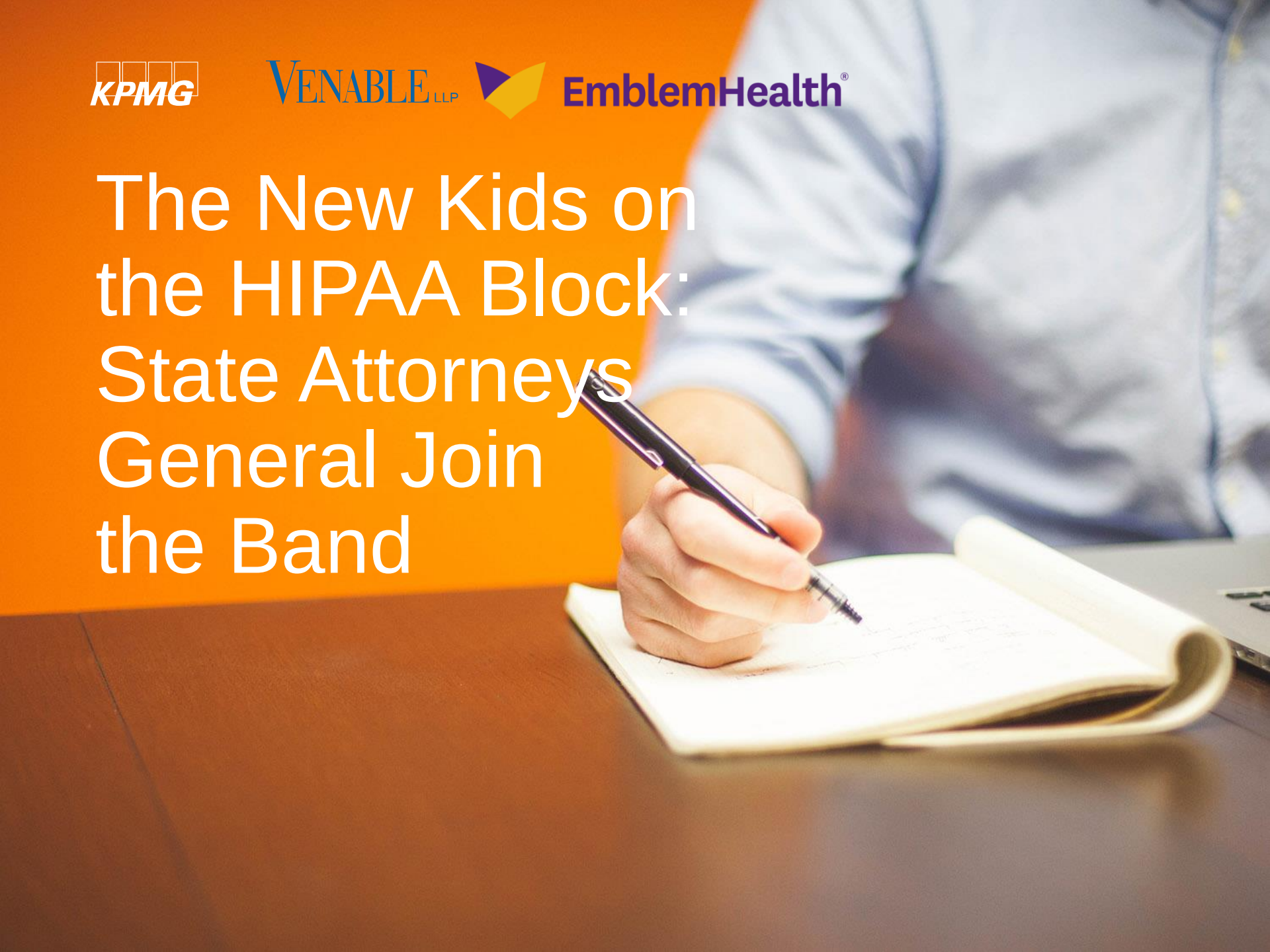
KPMG VENABLE LLP EmblemHealth

The New Kids on the HIPAA Block: State Attorneys General Join the Band



Overview

Introduction

***Since You Walked into My Life*: Overview of recent HIPAA Enforcement activities**

***Step by Step*: Life cycle of a State Attorney General Action**

***Hangin' Tough*: How a Breach Can Improve your Privacy Program**

Team Profiles

Thora Johnson, Partner, Venable LLP

Thora Johnson is a partner and the head of Venable's health care practice. She provides counsel on regulatory, compliance, tax, and business matters that are impacting healthcare providers, hospitals, continuing care retirement communities, health insurers, group health plans, pharmaceutical and medical device companies, and health information technology companies. She regularly structures HIPAA compliance and incident response programs for healthcare providers, health plans, and their business associates. She provides guidance on the intersection of HIPAA and state laws governing the confidentiality of medical records.

Joseph Lurin, VP Corporate Compliance & Privacy Official, EmblemHealth

Joseph Lurin is the Vice President, Corporate Compliance for the EmblemHealth Family of Companies. Joseph serves as the company's Privacy Officer and is responsible for leading the company's privacy strategy. He received a BA from the University of Massachusetts, and an MBA in Health Care Administration from Baruch College. Joseph is a Certified Information Privacy Professional (CIPP/US) and is Certified in Healthcare Compliance (CHC).

Jaime Pego, Managing Director, KPMG

Jaime Pego is a Managing Director in KPMG's Forensic Risk & Consulting Practice. She has more than 15 years of experience delivering compliance advisory services, including HIPAA risk assessments, billing/coding reviews, and compliance program effectiveness reviews, to a wide range of healthcare clients. She also serves as the National HIPAA Privacy Managing Director at KPMG and worked on the engagement with the Office for Civil Rights to develop the HIPAA Privacy Audit Protocol. Jaime graduated from Seton Hall Law School with a concentration in health law, and is a licensed attorney in New York and New Jersey.

Since You Walked into My Life

Overview of State HIPAA Enforcement

In recent years, States Attorney General ("SAGs") have begun to exercise their authority to enforce the Health Insurance Portability and Accountability Act ("HIPAA"). Previously, SAGs issued financial penalties solely for violations of state privacy or security laws, and left HIPAA enforcement to the Office for Civil Rights.

Covered entities and business associates now must be aware of possible state enforcement for violations of the HIPAA Privacy and Security Rule. In 2018, the total number of state settlements exceeded the total number federal settlements.

Health Information Technology for Clinical and Economic Health Act ("HITECH")

- Established in 2009 as part of the American Recovery and Reinvestment Act.
- Granted SAGs authority to bring civil actions on behalf of state residents for violations of the HIPAA Privacy and Security Rule.
- Covered entities and business associates that violate HIPAA may now be subject to penalties from both the Office for Civil Rights as well as the SAG in their respective states.

Office for Civil Rights ("OCR")

- OCR assists SAGs in investigating state civil actions by providing information about pending or concluded OCR actions.
- OCR developed HIPAA enforcement training materials that are designed to assist SAGs implement their new authority.
- SAGs must serve OCR with the state complaint at least 48 hours prior to bringing action.

2018 HIPAA Settlements

- OCR reached 10 federal settlements in 2018 with covered entities and business associates, as well as one judgment, totaling $28.7M (an increase from 2017).
- SAGs reached 12 state settlements with SAGs in 2018, totaling $3.6M. While the number of settlements with SAGs increased from 2017, the total settlement amount was similar.
- The SAGs in the following states instituted actions and negotiated settlements in 2018: New Jersey, New York, Massachusetts, Connecticut, Washington, and D.C.

Sample State Actions

Aetna Privacy Breach

- Aetna entered into a $1.15M settlement with the NY SAG for inappropriately disclosing (i) HIV/AIDS information related to approximately 2500 patients, and (ii) atrial fibrillation information related to about 1600 patients.
- The sensitive information was visible through the envelope windows of members mailings.
- The disclosure of the HIV/AIDS information also led to related settlements with the Connecticut, D.C., and New Jersey SAGs (for $100K, $175K, and $365K respectively), since affected patients resided in these states as well.

EmblemHealth Privacy Breach

- EmblemHealth entered into a $575,000 settlement with the NY SAG, as well as a $100,000 settlement with the NJ SAG, for inadvertently disclosing the Medicare health insurance claim number ("HICN") of over 80,000 members.
- The HICN (which mirrors the social security numbers) were visible on a label that was included on the envelopes of member mailings.

Medical Transcription Security Breach

- Best Medical Transcription, a business associate to a physician medical group, entered into a $200K settlement with the NJ SAG for a security breach involving the medical records of over 1500 patients.
- Physician notes were inadvertently exposed when the password protection of the medical transcription company's website was inadvertently removed during a software upgrade.
- The physician medical group also entered into a settlement with the NJ SAG for $417,000 for the same violation of Best Medical Transcription, despite the fact that it maintained a business associate agreement with the vendor.

UMass Memorial Health Care Data Breach

- UMass Memorial Health Care, along with an affiliated physician group, jointly entered into a $230K settlement with the Massachusetts SAG for a security breach involving the health information of over 15,000 patients.
- Social security numbers, health insurance information, and clinical information was accessed by two employees for purposes of opening cell phone and credit card accounts.
- UMass was aware of the employees' misconduct, but failed to investigate and take action in a timely manner.

Multi-State Litigation

First Multi-State Data Breach Lawsuit

1 ***In the first case of its kind, 16 SAGs jointly filed a data breach lawsuit against Medical Informatics Engineering and its subsidiary, NoMoreClipboard LLC, an electronic health records company, on behalf of their state residents that were affected.***

2 ***This case was filed in a federal district court in Indiana by the SAGs of the following states, alleging violations of HIPAA: (i) Indiana, (ii) Arizona, (iii) Arkansas, (iv) Florida, (v) Iowa, (vi) Kansas, (vii) Kentucky, (viii) Louisiana, (ix) Minnesota, (x) Nebraska, (xi) North Carolina, (xii) Wisconsin.***

3 ***The lawsuit concerns a May 2015 data breach in which hackers allegedly stole health information relating to 3.9 million individuals from the organizations' systems. According to the complaint, over a period of 19 days, hackers were able to infiltrate the organizations' computer systems. The stolen information allegedly included social security numbers, lab results, and medical record information.***

4 ***In May 2019, the Company settled with OCR for $100,000 and with the states for $900,000 for a total of $1 million. The Company also committed to a two-year corrective action plan to resolve potential violations of the HIPAA Privacy and Security Rules.***

Multi State Action

Premera Blue Cross Blue Shield Data Breach

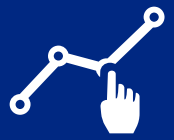
- In July 2019, Premera Blue Cross Blue Shield entered into a **$10 million settlement with 30 states** to resolve allegations that Premera's inadequate security measures left its network vulnerable to hacking and exposed consumers' Social Security numbers and sensitive health information.
- From May 5, 2014 through March 6, 2015, a hacker had unauthorized access to the Premera network containing private health information, Social Security numbers, bank account information, names, addresses, phone numbers, dates of birth, member identification numbers and email addresses.
- The investigation found that Premera's inadequate data security exposed to a hacker the PHI/PII of more than 10.4 million insureds nationwide.
- A complaint filed with the settlement agreement asserts that Premera failed to meet its obligations under HIPAA and violated state consumer protection laws by not addressing known cybersecurity vulnerabilities.
  - The complaint also asserts that Premera misled consumers nationwide about its privacy practices in the aftermath of the data breach. After the breach became public, Premera's call center agents told consumers there was no reason to believe that any of your information was accessed or misused even though multiple security experts and auditors warned the company of its security vulnerabilities prior to the breach.
- Separate class action litigation involving the breach resulted in a proposed settlement in June 2019 that would result in a $32 million recovery for affected consumers, and would require Premera to make $42 million in cybersecurity upgrades.

Enforcement Considerations

Due to differing priorities and considerations, the OCR and SAGs often elect to pursue different HIPAA cases. The settlements entered into by the OCR and SAGs in 2018 all involved different underlying breaches.

OCR Considerations

- Each OCR settlement in 2018 involved organizations that failed to conduct thorough risk assessments that satisfied the standards of the HIPAA Security Rule.
- In the event of a breach, the OCR considers whether the organization has considered the root causes of the underlying issue.
- The OCR also considers the organization's response to the breach once identified, including the mitigation activities that were completed and the training that was provided to the workforce to address the issue.
- The OCR is less focused on one-off, inadvertent mistakes (i.e. mailing errors), and more interested in pursuing cases that involve systemic issues of non-compliance.



SAG Considerations

- SAGs are elected positions in most states (43 out of 50), so they are more susceptible to public pressures in the event of a breach that affects state residents.
- Due to these political pressures, SAGs may be more willing to pursue those breaches that involve one-off mailing mistakes, especially if the breach is well publicized and prevalent in the media.
- In recent years, SAGs have taken a more active role in enforcing HIPAA breaches that were not previously pursued by the OCR.
- SAGs are not as familiar with the practical application and enforcement of the privacy and security laws in the health care industry.

Potential Corrective Actions

Agreements with the SAGs detail the corrective actions and monitoring activities that entities must complete in order to comply with the terms of the settlements. These may include:

Implementing policy, protocol, and training reforms related to safeguarding protected health information.

Engaging third party vendors to evaluate the progress of remediation activities and prepare a report on compliance with the settlement agreement terms.

Conducting privacy and security risk analyses (internally or through the use of a third party vendor) related to the applicable business processes, including member mailing processes.

Reviewing and updating privacy and security policies and procedures.

Improving training materials related to applicable privacy and security business processes.

Step by Step

Life Cycle of a SAG Action

Step 1: The Calm Before the Storm

- Engage legal counsel … YOU WILL NEED IT!
- Check the respective state's requirements regarding providing notice to the SAG and OCR.
- Check individual state requirements for member notification and identify theft protection.
- Craft your message and document it consistently across jurisdictions.
- Determine if you need a vendor to issue member notices, operate a call center, or provide identify theft protection services.

Step 1a: Remediate Early and Often

- If employee discipline is appropriate, work with Human Resources to document it.
- Take this opportunity to tighten your organization's policies and procedures, especially surrounding the process that caused the breach.
- Be proactive – Retrain employees and issue privacy communications across the organization.
- Report the incident to your Governing Body.

Life Cycle of a SAG Action (continued)

Step 2: All Eyes on You

- Investigations typically start with a request for information … and another … and another.
- Categories of information requested will vary by state – be sure to keep your story consistent and your materials organized.
- Maintain documentation of all remediation efforts.
- Respond timely and completely.
- Ask for more time if you need it.

Step 3: Let the Games Begin

- Meet face-to-face to advance your arguments and educate non-OCR and non-health care industry personnel.
- REMEMBER: These are lawyers … "Everything you say can and will be used against you."
- Don't bid against yourself – get a first draft.
- "Same bat time, same bat channel" – If you are dealing with multiple SAGs, sell them the same deal to maximize remediation efforts.

Hangin' Tough

How a Breach Can Improve your Privacy Program

Although settlements with SAGs have financial and reputational repercussions, organizations can also use them as opportunities to improve the long term health of their privacy and security programs in a variety of ways.

Talk To Me Goose: Increase the frequency of your privacy communications.

Put It In Writing: Revise your organization's policies and procedures to include guidance on identified gaps, and review business associate agreements.

Teach Your Children Well: Revise your annual training curriculum or implement additional department modules to target gap areas.

Bare Your Soul: A risk assessment is useful to find gaps and vulnerabilities.

Moving your Program Forward

Annual Preparation Activities

Organizations should conduct the following on an annual basis to ensure that they are in position to respond as necessary in the event of an investigation:

Develop HIPAA Audit and Investigation Response Repository

- A HIPAA Audit and Investigation Response Repository that contains key policies, procedures, and control documentation should be maintained for easy response to investigative demands.
- Organizations should review the Repository on an annual basis to confirm that all documents are up-to-date and representative of current HIPAA practices within the organization.

Develop HIPAA Audit and Investigation Response Team Stakeholder List

- A HIPAA Audit and Investigation Response Team Stakeholder List should be maintained and reviewed periodically to ensure appropriate stakeholders are identified and still working for the organization.
  - Make updates based on changes in workforce staff (e.g., terminations, transfers) and changes to key stakeholder roles and responsibilities (e.g., if a role is no longer responsible for HIPAA controls).
  - These individuals will play a critical role in any response to investigations by OCR or SAGs.

Perform Annual HIPAA Risk Assessment or Mock Audit

- An enterprise-wide HIPAA Privacy and Security Risk Assessment or Mock Audit should be conducted on an annual basis to assess current HIPAA controls against regulations, identify any gaps in existing controls, and provide recommendations to close the gaps.
- These activities will serve to identify vulnerabilities, and the resulting outputs can be provided to the regulators following an incident or breach to reflect the organization's proactive efforts to assess its control environment.

Perform Periodic Security/Privacy Walkthroughs

- A HIPAA Physical Safeguards Walkthrough Checklist should be developed to identify physical safeguard requirements.
- The Information Security or Privacy Office should use the HIPAA Physical Safeguards Walkthrough Checklist to conduct periodic walkthroughs of select physical sites on a periodic basis.
  - Organizations should review and document the findings of walkthroughs to identify trends, opportunities for improvement, and/or additional training opportunities.

Conclusion

Takeaways from NKOTB

REMEMBER…. Take a page from NKOTB when managing your privacy program and response to regulators:

Write Great Songs

- Develop your story for the regulators (with the assistance of counsel) and be prompt with the delivery.
- Enhance your internal message and improve your policies … AND GET THEM ON THE RADIO OFTEN!

Be Nimble on the Dance Floor

- Be equipped to educate non-health care focused investigators during the process.
- Be ready to document all remediation plans and activities … YOU NEED TO LOOK AS GOOD AS POSSIBLE AT THE END OF THE NIGHT!

Make a Dramatic Comeback

- DON'T LIVE IN THE PAST … Use the breach and subsequent investigation as an opportunity to improve your program and come back stronger than ever.

Contact Information

Please feel free to contact us with any questions:

Joseph Lurin
VP, Corporate Compliance, EmblemHealth
jlurin@emblemhealth.com
646-447-5203

Thora Johnson
Partner, Venable
tajohnson@venable.com
(410) 244-7747

Jaime Pego
Managing Director, KPMG
jpego@kpmg.com
(908) 416-1662