COSMOS
Navigate the Compliance Universe

Compliance Today - May 2022
State and federal HIPAA enforcement actions translate into compliance priorities

By Kara L. Hilburger, Esq., CIPP/US, and Alexis L. Rose, Esq., MPP, CHC

Kara L. Hilburger (khilburger@beckage.com) is Privacy Compliance & Digital Accessibility Team Leader, and **Alexis L. Rose** (arose@beckage.com) is Health Care Data Privacy Attorney at Beckage PLLC, Buffalo, NY.

Kara L. Hilburger

Alexis L. Rose

Since 2003, the U.S. Department of Health & Human Services Office for Civil Rights (OCR) has imposed more than 100 civil monetary penalties, totaling over $131 million, for violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).[1] Many recent enforcement actions have focused on right-of-access violations as part of OCR's Right of Access Initiative.[2] However, the costliest enforcement actions resulted from breaches of electronic protected health information (ePHI), with more than half of those enforcement actions in the past two years settling for $1 million or more.[3]

Since late 2019–early 2020, OCR has shifted its focus to right-of-access cases and responses to the COVID-19 public health emergency.[4] However, that does not mean covered entities or business associates should let their guard down regarding other areas of enforcement or be left unprepared when the public health emergency exceptions are lifted —OCR is still active, state attorneys general (state AGs) have become more active in recent years, and it is anticipated enforcement actions could become more common under the new OCR Director Lisa J. Pino, who has a background in cybersecurity.

State AGs have brought a growing number of HIPAA enforcement actions, often resulting in massive financial penalties for covered entities and business associates.[5] Under the Health Information Technology for Economic and Clinical Health Act, states may bring enforcement actions on behalf of their residents for HIPAA violations.[6] Recently, multistate actions have been on the rise, with state AGs working cooperatively to more efficiently investigate and enforce violations.[7] Not only have state enforcement actions been on the rise, but often states require more prescriptive corrective actions.

Taking an in-depth look at the 40 most recent OCR and state enforcement actions, several patterns emerge. This article outlines those enforcement patterns and evaluates best practices to address common deficiencies in areas such as governance, risk analysis and management, policies and procedures, and technical safeguards. Finally, the article provides tips on mitigating legal risk by prioritizing compliance initiatives based on recent trends in HIPAA enforcement actions.

Administrative enforcement themes

The state enforcement actions are unique due to their prescriptive nature. However, they often find similar deficiencies and areas for improvement as those areas outlined in OCR's enforcement actions. This section will outline the most common areas of enforcement focus. It will also highlight where the state enforcement actions

divert from OCR's enforcement actions around the same violations. Finally, it will provide some tips and best practices to help avoid noncompliance with these areas of high enforcement risk.

Governance

Establishing a data governance structure that works for your organization is critical to a successful compliance program. Covered entities and business associates are required to designate a security officer who is responsible for overseeing its organization's compliance with the HIPAA Security Rule.[8] Covered entities must also designate a privacy officer who is responsible for developing and implementing the organization's privacy practices, as well as an employee or office responsible for receiving privacy complaints.[9]

In addition to these key roles, it is imperative that covered entities designate and document the persons or offices responsible for processing requests for access, particularly in light of the rise of enforcement actions focusing on right-of-access violations.[10] Smaller covered entities can delegate this role to the privacy officer. Medium to larger-sized organizations generally delegate this responsibility to the health information management department, with oversight from the privacy or compliance officer.

Moreover, organizations should consider designating specific individuals who will participate in the organization's incident response team. Key roles and responsibilities should be clearly outlined in the incident response plan.

Covered entities and business associates should also consider potential obligations under state law related to governance. For example, at least one enforcement action distinguished between a chief information security officer (CISO) and the HIPAA privacy and security officer (HPSO).[11] The enforcement action stated that the CISO should be an "executive or officer" and regularly report to the CEO, the HPSO, executive staff, and the board of directors. State AGs require this officer to have the appropriate background and expertise to implement, maintain, and monitor the organization's information security and privacy program.

In addition to personnel requirements, state AGs have also focused on whether privacy and security programs had proper resources. Specifically, at least one state enforcement action required that organizations "budget such that [the] Information Security Program receives the resources and support reasonably necessary to function as intended."[12] It is important that leadership provide enough human capital and monetary resources for the privacy officer and security officer to properly run a HIPAA compliance program. It is also recommended that the CISO, privacy officer, and security officer have the proper authority to implement the HIPAA compliance program, including access to CEO and, in some cases, the board or a committee.

Risk analysis

When a covered entity or business associate reports a breach, the subsequent investigation will invariably include an examination of the organization's risk analysis and risk management plan. As such, failure to conduct an accurate, enterprise-wide risk analysis and implement risk-mitigating measures are two of the most common HIPAA violations in both OCR and state enforcement actions. Even though the HIPAA Security Rule does not specify how often to conduct a risk analysis, industry best practice is to conduct a risk analysis at least once annually and more often in response to environmental and operational changes.[13] Organizations may need to update their policies and procedures in response to any newly identified risks.

A risk analysis should identify all risks to the security, privacy, and integrity of protected health information (PHI). As part of this process, it is necessary to develop and maintain a complete inventory of all electronic

equipment, data systems, and applications that contain or store ePHI. Often, a risk analysis will not only identify risks but rank them based on the probability of occurrence and severity of harm (i.e., reputational harm, financial harm, and regulatory fines or legal liability). Covered entities and business associates should mitigate the security threats and vulnerabilities identified in the risk analysis by implementing a risk management plan. Although organizations may be unable to mitigate all identified risks, they should take steps to mitigate the highest-ranked risks and identify existing controls in place to mitigate risks that are not eliminated. All these compliance steps should be documented, including a timeline for implementation, and detail the personnel responsible for implementation and evaluation.

Written policies and procedures

Documentation is key to HIPAA compliance and includes the use of enterprise-wide policies and procedures that conform to federal standards. Policies and procedures are always an area of focus in OCR resolution agreements. Often, OCR and state agencies will require HIPAA violators to submit their policies and procedures for review and approval as part of resolution agreements. Covered entities and business associates should assess, update, and make necessary revisions to their policies and procedures at least annually. Changes to an organization's privacy and security practices and environmental changes should be reflected with immediate revisions.

Organizations must promptly distribute their policies and procedures to all workforce members. New employees should receive copies of these policies and procedures, and current employees should be notified of changes to HIPAA policies and procedures. Often organizations will have employees sign an acknowledgment that they have read and understood the policies and procedures, but it is also important they receive training on policies and procedures. Policies that affect the entire staff should also be easily accessible to staff for reference and review.

Following a breach or other HIPAA violation, organizations should always review existing policies and evaluate whether revisions would help mitigate the risk of similar violations. If this is done quickly and properly, this can be used as a mitigating factor when negotiating penalties with OCR or an attorney general's office.[14]

Training

In several recent HIPAA enforcement actions, the conduct of individual workforce members was the primary cause of the resulting breach of PHI. As such, the requirement that covered entities and business associates provide privacy and security awareness training for all workforce members is crucial.[15] It is best practice that workforce members who have access to PHI receive training at least annually, with new workforce members receiving training as soon as possible upon hire, preferably within 14 days but no later than 30 days of hire. Similar to the requirements for distributing policies and procedures, organizations should require their workforce members to certify, either in electronic or written form, that they attended and completed training. The content of the training should be reviewed at least annually and updated, as needed, to address changes in federal law or agency guidance.

In some of the state enforcement actions, the organization was required to implement training on specific topics, including anti-phishing.[16] In addition to the annual HIPAA training, covered entities and business associates should also provide periodic refreshers about HIPAA through tools like monthly newsletters or quarterly HIPAA safety reminders. Organizations should also consider retraining workforce members who violate HIPAA policies, in addition to disciplinary action consistent with the organization's sanction policy.

Business associate agreements

OCR has brought multiple enforcement actions over the past few years where a covered entity failed to have a

business associate agreement in place. Additionally, covered entities have been found in violation of HIPAA when they failed to obtain reasonable assurances from the vendor that it has information security safeguards in place that meet HIPAA standards.[17] When covered entities or business associates share PHI with vendors, they must share only the minimum necessary amount of PHI for the vendor to fulfill its obligations.

Compliance related to business associate agreements should be broken down into three parts.

1. Strong vendor management is important to any HIPAA compliance program. A covered entity or business associate should have procedures in place to identify vendors that require access to PHI to provide business associate services. The organization must establish and implement procedures to confirm that business associate agreements are executed prior to the disclosure of PHI. It is also important that any staff that interface with the vendor have appropriate HIPAA training.
2. Covered entities and business associates must conduct due diligence on all business associates before and during the contractual relationship. This may include information security questionnaires, review of policies, certifications of compliance, and/or audits of the vendor's compliance program.
3. Finally, it is important to have safeguards in place that restrict access to PHI to the minimum amount of PHI and authorized vendor personnel necessary to provide services.

Documentation of business associate agreements as well as documentation of due diligence and monitoring should be maintained for at least six years beyond the date when the contractual relationship is terminated.[18]

Technical compliance requirements

Although both OCR and the state AGs' offices have focused enforcement actions on the technological safeguards required under HIPAA, the state enforcement actions are often unique in interpretation and prescriptiveness. OCR has long taken the stance that although there are specific safeguards required under the HIPAA Security Rule, it is meant to be flexible based on an organization's size, resources, and complexity. OCR focuses on compliance with technical requirements in the Security Rule but generally does not require organizations to adopt specific standards like the ones from the National Institute of Standards and Technology or specific software like Barracuda. State AGs often take a more prescriptive approach, sometimes requiring covered entities and business associates to meet specific standards in addition to the HIPAA Security Rule. In one enforcement action out of New Jersey, the attorney general required the organization to become certified in Health Information Trust Alliance (HITRUST).[19] Additionally, some resolution agreements have required specific means to accomplish a particular safeguard, such as implementing Barracuda for email access control and implementing a security information and event monitoring solution for network activity monitoring.[20] Although these are all best practices, it brings a new level of specificity to HIPAA enforcement actions and remediation measures.

Another theme that was observed related to the more technical components of the HIPAA Security Rule is the treatment of addressable safeguards. The HIPAA Security Rule designates safeguards as either required or addressable.[21] Covered entities and business associates must implement the required safeguards and must, at a minimum, assess the ability to implement an addressable safeguard. Covered entities and business associates should not treat addressable safeguards as optional and should only forgo them if they can document a compelling reason the organization could not implement the safeguard.

However, in many of the reviewed enforcement actions, OCR and the state AGs have issued significant fines for noncompliance with addressable safeguards. For example, both OCR and state AGs have issued significant fines

for the lack of encryption of ePHI.[22] Even though encryption is technically an addressable safeguard, these actions reinforce that addressable safeguards should not be treated as optional. Password management is another example of an addressable safeguard that has been the focus of several enforcement actions.[23] Organizations should also be sure to implement common-sense password management requirements, such as using strong passwords, rotating passwords, implementing multifactor authentication, and ensuring that stored passwords are protected from unauthorized access.