haynesboone

March 6, 2015

Anthem's Data Breach Impacts Many Anthem and Non-Anthem Plans: Necessary Employer Actions Now

On January 29, 2015, Anthem, Inc., an insurer and service provider for many employer-sponsored health plans, discovered a cyber-attack that compromised the personal health plan data of millions of current and former participants in Anthem's affiliated health plans, as well as many independent Blue Cross and Blue Shield ("BCBS") plans where Anthem processed claims through the "BlueCard" program. Anthem's investigation to date indicates names, dates of birth, ID numbers, social security numbers, home addresses, phone numbers, email addresses, and employment information were accessed. Due to the massive scope of this breach and the relationships between Anthem and other health plans that are not labeled Anthem or BCBS, employers should not assume that their health plans were unaffected if they are not directly contracting with Anthem or BCBS.

As discussed below, an employer should (1) determine if the Anthem breach affects any of its employees and ensure that all obligations under federal and state law are being met, (2) take other steps to control HIPAA-related risks affecting its health plan, and (3) understand the ERISA fiduciary duties associated with such compliance efforts. Even if your plan was not impacted by the Anthem breach, the compliance pointers set out below should still be considered now because your plan may not be as fortunate next time – and there will likely be a next time.

Anthem-Breach Action Items

If an employer has not done so already, it should contact the insurer or third party administrator of its health plan and ask if any of the participants or former participants in its health plan were affected by the Anthem breach. If so, the employer should:

- Alert affected employees that calls or emails purporting to be from Anthem are scams. Anthem has stated that affected individuals will receive information from Anthem via mail.
- Direct affected employees to Anthem's toll-free hotline (877) 263-7995 and to *www.anthemfacts.com* for answers to frequently asked questions, as well as for information regarding credit monitoring and identity theft protection services provided by Anthem.
- Contact legal counsel to determine what notifications are required under state or federal law.
    - Fully-insured plans: Receive written confirmation from the insurer that it will comply with any breach notification requirements under HIPAA.
    - Fully-insured plans: Request evidence from the insurer that all required notifications were properly made. The employer's group health plan (*i.e.*, as an entity separate from the insurance policy) is also a "covered entity" subject to the HIPAA breach notification

© 2015 Haynes and Boone, LLP

requirements, which means the plan could be liable if notifications were not made by the insurer.

- Self-funded plans: Review HIPAA business associate agreements ("BAAs") to determine if the plan has delegated breach notification responsibility to the third party administrator. There have been reports that the U.S. Department of Health and Human Services ("HHS") wants Anthem to handle the breach notification requirements under HIPAA. If that is the case, affected employers would be well-advised to contact their third party administrators if they have not delegated breach notification responsibilities to another party under their BAAs.
- Fully-insured or self-funded plans: Evaluate whether any notifications are required under applicable state laws, if these notifications can and/or will be made by the insurer or third party administrator, and document satisfaction of such requirements.

- Employers should also document the incident in accordance with the requirements of their own HIPAA breach policies and procedures.

Enforcement Actions

The cyber-attack on Anthem may have resulted in a breach under HIPAA that requires notification to HHS, as well as notification to affected individuals and the media. HHS must be notified within 60 days of any breach of unsecured protected health information ("PHI") that affects 500 or more individuals in a state or jurisdiction, and annually of breaches affecting fewer individuals. Employers should be aware that HHS notifications of breaches affecting at least 500 individuals are public and could gain media attention. In addition, such notifications may trigger an investigation by HHS into the covered entity's compliance with HIPAA's security and privacy rules. HHS investigations may also be triggered by an employee complaint to HHS.

If HHS finds during its investigation that the covered entity was compliant with HIPAA, the breach was an isolated incident, and appropriate measures are in place to prevent a similar breach in the future, then HHS may close the case without requiring a resolution agreement or settlement payment.

However, if the covered entity's current HIPAA compliance efforts are found lacking, HHS may require a resolution agreement to resolve the violations. To date, HHS has entered into over 20 resolution agreements with covered entities. These resolution agreements are public and may require covered entities to pay a resolution amount, perform certain obligations (*e.g.*, training), and make periodic reports to HHS, generally for a period of three years. For example, HHS entered into a resolution agreement with Affinity Health Plan, Inc. that included payment of $1,215,780 to HHS. Affinity impermissibly disclosed PHI when it returned copy machines to a leasing company without erasing the data contained on the copiers' hard drives. Affinity also failed to include the leased copy machines in its HIPAA security risk assessment.

© 2015 Haynes and Boone, LLP

A $1 million settlement is not extraordinary. The final HIPAA omnibus regulations include the HITECH Act's tougher penalties for violations of HIPAA, which range from $100 to $50,000 per violation (i.e., per affected individual) depending on whether the person knew (or by exercising reasonable care should have known) that he was violating HIPAA, or acted with willful neglect. The maximum penalty for identical violations in a calendar year is $1.5 million. If more than one HIPAA requirement was violated, penalties could surpass $1.5 million. HHS may share information found during its investigations and compliance reviews with other law enforcement agencies.

In addition to investigations initiated by breach notifications or complaints by individuals, HHS also conducts random audits of covered entities, including employer plans. HHS conducted a pilot audit program in 2012 and is expected to conduct a second round of audits in 2015.

Controlling Risk under HIPAA

There are a number of steps that employers can take to reduce the likelihood that they will be the subject of a data breach or face penalties during a government audit or investigation. The time and expense to fully resolve a breach under applicable state and federal rules, not to mention any resultant damaging publicity, could be enormous. These action steps include the following:

- Ensure that the policies and procedures required under HIPAA privacy and security rules are compliant and up-to-date, *e.g.*, have such documents been revised for changes made by the final omnibus HIPAA regulations?
- Verify the Notice of Privacy Practices is up-to-date, accurately reflects how the health plan uses and discloses PHI, and is being distributed in the time and manner required by HIPAA.
- Review current BAAs to ensure that they (1) have been revised for the final omnibus HIPAA regulations, (2) include adequate indemnification provisions (or these are included in the related services agreement), and (3) accurately reflect the employer's intentions with respect to the delegation of breach notification responsibilities. BAAs *are not* boilerplate documents. They need to be carefully reviewed and negotiated like any other important contract, such as a services agreement with a third-party plan administrator.
- Train all members of the workforce who may have access to PHI on its proper handling, as well as the other HIPAA security and privacy requirements that are relevant to the employee's position.
- Perform a security risk assessment to determine where there may be a risk of an impermissible use or disclosure of PHI. The federal government has provided a downloadable security risk assessment tool that can be used to perform this risk assessment: http://www.healthit.gov/providers-professionals/security-risk-assessment. The risk assessment should include coordination with the employer's IT department to evaluate compliance with HIPAA's security rules for electronic PHI.

© 2015 Haynes and Boone, LLP

- Ensure that adequate insurance coverage is in effect to cover losses resulting from cyber-attacks and HIPAA violations. Cyber-security policies are increasingly common components of employers' risk control programs.

Related ERISA Fiduciary Obligations

Each employer-sponsored, group health plan that is subject to ERISA must have one or more responsible fiduciaries who are required by ERISA to act in the best interest of the plan's participants. The plan's fiduciaries must also ensure that the plan's terms are being followed and comply with all applicable laws and regulations. Furthermore, the responsible plan fiduciary must ensure compliance with both governmental and participant reporting and disclosure requirements. Plan fiduciaries may include the employer, as well as the plan's committee, claims administrator, and its HIPAA privacy and security officers. Under ERISA, fiduciary status is a functional test based on the person's authority or control over the plan or its assets.

Group health plan fiduciaries have a responsibility to act prudently to prevent PHI from being impermissibly disclosed or compromised. In the event of a breach, the responsible plan fiduciary must stay informed and keep participants informed. In that regard, the fiduciary should recognize that all correspondence to plan participants may likely be fiduciary communications under ERISA. The responsible plan fiduciary should advocate for participants and work to minimize any harm to them and the plan itself that may result from a breach. The fiduciary must also keep a record of actions it takes to investigate and remedy the breach.

The U.S. Department of Labor enforces ERISA and may bring an action against a fiduciary who allegedly breaches a fiduciary duty to the plan. Plan participants may also sue a plan fiduciary for a fiduciary breach. In either case, a fiduciary who fails to take timely action to prevent a breach, or to minimize harm to the plan and its participants resulting from a breach, may be exposed to personal liability under ERISA.

An employer should ensure that plan fiduciaries are properly trained and understand their responsibilities under ERISA. The employer may indemnify the plan's fiduciaries, and ERISA fiduciary liability and errors or omissions insurance coverage may be obtained to protect the plan and its fiduciaries from damages and expenses.

Contact Information

Hackers are out there, and mistakes happen. Real penalties are being assessed. Employers should prepare now to reduce the risk of impermissible uses and disclosures of PHI, as well as to establish policies to mitigate damages if a breach does occur.

© 2015 Haynes and Boone, LLP

haynesboone

For more information, please contact:

Jesse Gelsomini
713.547.2323
jesse.gelsomini@haynesboone.com

Kirsten Garcia
214.651.5171
kirsten.garcia@haynesboone.com

This publication does not contain legal advice, should in no way be taken as an indication of future legal results, and is provided for educational and informational purposes only. You should not act on any information provided without consulting legal counsel. Any advice contained in this communication is not intended to be used, and cannot be used, by any person to avoid penalties under federal law, and such advice cannot be quoted or referenced to promote or market to another party any transaction or matter addressed in this communication.

© 2015 Haynes and Boone, LLP