HUSCH BLACKWELL

April 25, 2015

DATA SECURITY FOR EMPLOYER HEALTH PLANS IN THE WAKE OF ANTHEM AND PREMERA

Peter Sloan

Pete Enko

Anthem's data breach announcement in February,[1] followed by the March disclosure by Premera Blue Cross of a strikingly similar cyber-attack,[2] sent waves of alarm through both the health care industry and the employer health plan community.

The scale of these companion breaches is astonishing. With current estimates of 78.8 million affected individuals for Anthem and 11 million for Premera, the collective size ranks among the largest data breaches in history – involving more individuals than the Target, Home Depot, Sony, or JP Morgan Chase breaches.[3]

As HIPAA breaches, Anthem and Premera are twin tsunamis. The HHS Office of Civil Rights' (OCR) public listing of HIPAA breaches affecting 500 or more persons, from 2009 to the present, includes a total of 909 security breaches reported to OCR by HIPAA-covered medical providers, healthcare clearing houses, and health plans. Until now, health plans have been a backwater of HIPAA breaches, comprising only 13 percent of these OCR-reported incidents. But the Anthem and Premera breaches by themselves account for more than four-fifths of the 110 million total individuals affected by all OCR-reported HIPAA breaches over the last six years.[4]

Anthem and Premera signal a sea change in the threat environment for health plans, a new reality that requires a fresh look at data security. Prudent employers with self-funded group health plans should take that fresh look now, by strengthening the data security provisions in their services agreements with third-party plan administrators (TPAs), and also by updating their HIPAA-required security risk assessments.

It's Time for BAA 2.0

In the days following Anthem's breach announcement, employer benefit managers and in-house legal counsel were adrift.

Who would be responsible for making HIPAA and state law notifications to the thousands of affected members of their group health plans? What about required notifications to federal or state regulators, or to the media? And what about liabilities and exposures for any future claims? For answers, employers pulled out their administrative services agreements and BAAs with Anthem-affiliated TPAs… only to find no clear provisions for the Anthem scenario.

BAAs should reflect the security requirements, response delegations, and allocations of breach exposures appropriate for this new threat environment.

Under HIPAA, a self-funded health plan is a Covered Entity, responsible for making the required breach notifications to affected individuals, the media, and OCR.[5] The TPA is the HIPAA Business Associate, responsible under HIPAA rules solely for notifying the Covered Entity of the protected health information (PHI) breach.[6] And to the extent that state breach notification laws are applicable,[7] notification responsibilities generally rest upon the entity that "owns or licenses" the individuals' personally identifiable information (PII).[8]

Breach notification obligations may be delegated contractually. OCR's HIPAA guidance indicates that a Covered Entity can assign to its Business Associate the making of required notifications regarding breaches involving the Business Associate.[9] Similarly, under state PII breach notification laws, the entity that owns or licenses PII can contractually require another to make notifications on its behalf.

In the Anthem aftermath, many employers found (1) no delegations for making HIPAA notifications and (2) no provisions for security, breach exposures, and notification responsibilities regarding PII. In a pre-Anthem/Premera world, that makes sense. Going forward, however, health plan BAAs should reflect the security requirements, breach notification and response delegations, and allocations of breach liabilities in a manner appropriate for this new threat environment.

Accordingly, BAA 2.0 should:

Address the security of both PHI and PII. TPAs inevitably will have custody of PII on behalf of group health plans. At least nine states impose affirmative data security program requirements on entities that maintain PII. Rather than merely obligating the TPA to comply with HIPAA, BAAs should also require that TPAs comply with state security program mandates and establish prudent safeguards for PII.

Clarify response obligations for both PHI and PII breaches. The BAA should spell out the responsibilities of the plan and the TPA in the event of a data breach under both HIPAA and state breach notification laws. Delegations of responsibility for notifying individuals, regulators, and others should be clearly expressed.

Allocate liabilities and indemnities for breach response. The TPA's security and breach response obligations should be well-linked to the liability and indemnification provisions of the administrative services agreement and the BAA. The employer should consider the feasibility of requiring that the TPA maintain adequate cyber insurance, with the plan as an endorsed insured under the policy.

Many factors beyond data security are involved when an employer selects a TPA for its group health plans. Cost is, of course, centrally important. But the data security posture of the TPA should not be an afterthought, particularly if the TPA has had a history of data security incidents.[10]

Employers can point to the Anthem and Premera breaches, along with any known, prior security incidents involving the TPA, when negotiating toward a more robust BAA. Employers should also consider asking for documentation that provides reasonable assurance about the TPA's security measures, such as a SOC 2 audit report on service provider security controls.

It's Time for an Updated Security Risk Assessment

HIPAA requires health plans to conduct a security risk assessment,[11] and to reassess the adequacy of security controls at least annually and whenever changed circumstances warrant.[12] Results of the risk assessment and periodic evaluations must be documented in writing and retained for at least six years after no longer in effect.[13]

When a breach triggers an OCR investigation, one of the first items requested by OCR will be a copy of the up-to-date security risk assessment and most recent periodic evaluation.

Employers with small- to medium-sized health plans might be tempted to view themselves as too insignificant for hacking or other security intrusions. But Social Security numbers and health data are far more valuable on the black market than the cardholder data targeted in large retailer cyber-attacks.[14]

Moreover, the employer health plan may not be the hackers' ultimate objective. Speaking of "too small of a target," the same could have been said for HVAC service provider Fazio Mechanical – reportedly the hackers' entry point into retailer Target's network through a supplier portal.[15] Similarly, most benefits managers use a portal to connect with their TPA's data systems for plan administration.

Group health plan employers should update their security risk assessments now, in light of the Anthem and Premera breaches and the current threat environment.

A compliant security risk assessment is not merely a gap analysis comparing security practices to the security requirements of HIPAA and other applicable laws. It also includes the identification of threats, vulnerabilities, and risks to protected information, leading to the strengthening of the plan's data security posture. Documentation of the updated risk assessment is also crucial to protect the plan in the event of a data breach.

[1] *See* https://www.anthemfacts.com/. Anthem's website states that Anthem discovered the cyber-attack on January 29, 2015, and that Anthem believes the intrusion "happened over the course of several weeks beginning in early December 2014." *Id.*

[2] *See* http://premeraupdate.com/. The Premera Blue Cross website indicates that Premera discovered its cyber-attack on the same day as Anthem, January 29, 2015, and that "the initial attack occurred on May 5, 2014." Id.

[3] http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/.

[4] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

[5] 45 C.F.R. §§ 160.103 & 164.404–164.408.

[6] 45 C.F.R. §§ 160.103 & 164.410.

[7] Forty-seven states, the District of Columbia, and three US territories have PII breach notification laws, with various definitions of what constitutes PII and a breach requiring notifications. Most such statutes contain exceptions from notification requirements for entities subject to, and which comply with, breach notification requirements under HIPAA or those of other functional regulators.

[8] *See, e.g.,* Cal. Civ. Code § 1798.82(a).

[9] 78 Fed. Reg. 5650-51. *See also* http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html.

[10] For example, in July 2013 Anthem's corporate predecessor Wellmark Inc. entered into a $1.7 million resolution agreement with OCR regarding a security compromise of the names, dates of birth, addresses, Social Security Numbers, telephone numbers and health information of approximately 612,000 individuals during 2009 and 2010. http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/wellpoint-agreement.pdf.

[11] 45 CFR § 164.308(a)(1)(ii)(A).

[12] 45 CFR § 164.308(a)(8).

[13] 45 CFR § 164.316(b)(2)(i).

[14] *See* http://www.npr.org/blogs/alltechconsidered/2015/02/13/385901377/the-black-market-for-stolen-health-care-data.

[15] *See, e.g.,* http://krebsonsecurity.com/tag/fazio-mechanical-services/.

Contacts For Health Plan Data Security

Peter Sloan
Kansas City, MO
peter.sloan@huschblackwell.com
816.983.8150

Pete Enko
Kansas City, MO
peter.enko@huschblackwell.com
816.983.8312

About Our Data Security Team

Husch Blackwell's Data Security Team helps clients with security compliance and risk management, data breach response, and risk mitigation, including security risk assessments and breach response readiness planning. The team is part of the firm's Information Governance Group, which provides interdisciplinary expertise in Privacy, Data Security, and Information Management to help clients satisfy information compliance requirements and manage risk while maximizing information value.

About Our Firm

Husch Blackwell is an industry-focused, full-service litigation and business law firm with offices in 15 U.S. cities and in London. We represent national and global leaders in major industries including energy and natural resources; financial services; food and agribusiness; healthcare, life sciences and education; real estate, development and construction; and technology, manufacturing and transportation.