Advisory

FEBRUARY 2015

If you have any questions about this Advisory, please contact:

MICHELLE DEBARGE
860.297.3702
mdebarge@wiggin.com

SHERRY DOMINICK
203.498.4331
sdominick@wiggin.com

JOHN KENNEDY
203.363.7640
jkennedy@wiggin.com

JODY ERDFARB
203.363.7608
jerdfarb@wiggin.com

MICHAEL MCGINLEY
203.363.7638
mmcginley@wiggin.com

The Anthem Breach: What Affected Group Plans Should Be Thinking About

The massive data breach announced this week by health insurer Anthem, with up to 80 million consumer records exposed (including Social Security numbers, birthdays, e-mail addresses and employment-related data), brings a sudden world of pain to Anthem. Anthem is now scrambling to investigate the cause of the incident, meet regulatory obligations to notify consumers and regulators, and prepare for the onslaught of investigations and litigation. (The first class action suits were filed yesterday in federal courts in California and Alabama, and the Connecticut Attorney General's office yesterday announced an investigation into the incident.) According to the Frequently Asked Questions (FAQs) published on Anthem's website, all product lines of Anthem were affected by the breach.

But the fallout reaches beyond Anthem. Group health plans insured or administered by Anthem, and their sponsors, will need to be able to respond quickly and accurately to participants' questions about their personal data. Equally important, affected plans and their sponsors will also want to make sure they comply with their legal obligations to employees and understand their regulatory and contractual rights and obligations in light of the data security breach. Immediate concerns include the following:

- **Responding to participants concerns about privacy and identity theft.** Anthem has set up an informational website at www.anthemfacts.com. A FAQ for individuals who may have been affected by the breach is also posted at www.anthemfacts.com. While Anthem currently states that personal medical information was not compromised in the breach, it acknowledges that Social Security numbers, addresses, e-mail addresses and birthday information –key data bits for identity thieves and spammers – were likely compromised. Anthem has indicated that it will offer free credit monitoring and identity theft insurance to affected individuals who receive written notice from Anthem that their personal information may have been compromised.

Affected plans and employers should consider providing their own written communications to plan participants, including government information sources on how to protect against identity theft. Information concerning the availability of credit freezes (that allow consumers to place temporary holds on credit applications made in their name), fraud reports filed with consumer reporting agencies, and other basic identity theft protection measures should be provided. Connecticut and federal resources on these issues can be found at:

- Identity theft (Connecticut Attorney General's website): **http://www.ct.gov/ag/cwp/view.asp?A=2066&Q=292644**

CONTINUED ON NEXT PAGE

The Anthem Breach: What Affected Group Plans Should Be Thinking About

- Identity theft (Federal Trade Commission website): **http://www.consumer.ftc.gov/features/feature-0014-identity-theft**

However, given the current uncertainty regarding the scope of the Anthem breach, affected plan participants may wish to wait for more information before initiating a credit freeze.

- **Reviewing legal and contractual obligations.** Plan sponsors' legal responsibilities with respect to their health plans will differ depending on whether the group health plan is self-insured or fully insured by Anthem. Plan sponsors should review their legal obligations and contracts with Anthem to understand any rights and obligations that may be triggered as a result of the data breach. For example, plan sponsors will need to understand what HIPAA obligations Anthem has assumed as the third-party administrator. Even if Anthem is bound contractually to address breach notification and other HIPAA obligations, plan sponsors will need to determine what level of oversight they want to exercise since the health plan and its sponsor ultimately are responsible for compliance from a regulatory perspective. Relevant contracts may include plan documents, third party administrator service agreements and business associate agreements.

Questions to consider in reviewing such agreements include:

- What **notice and information rights** does the plan and its sponsor have vis a vis Anthem to know the identity of affected plan participants, obtain detailed information on the cause and scope of the breach, and review and approve the content of legally required notification letters that will be sent to plan participants, state and federal regulators, and the media?

- Does the contract address the parties' obligations regarding **notice under state data breach notification laws?** The reported size of the Anthem breach will likely implicate most of the 47 U.S. states that have such laws on the books.

- How does the contract address the **parties' respective obligations and liability concerning the security of personal data of plan participants**? Does the contract speak to specific data security requirements for personal data handled by the parties?

- Does the **plan have contractual obligations to cooperate with Anthem** in connection with a security incident or **does Anthem have contractual obligations to coordinate its response** with the plan?

- Does the contract address obligations for **cost reimbursement or indemnification related to data breaches**?

Wiggin and Dana's healthcare and cybersecurity practices have extensive experience in helping clients navigate compliance and liability issues in data breaches. Please direct questions to Michelle DeBarge, John Kennedy, Sherry Dominick and Mike McGinley.