Strafford

Presenting a live 90-minute webinar with interactive Q&A

Data Breaches in ERISA Benefit Plans: Prevention and Response

Navigating Regulations Governing Self and Fully Insured Plans;
Complying with Notice Requirements

THURSDAY, APRIL 23, 2015

1pm Eastern | 12pm Central | 11am Mountain | 10am Pacific

Today's faculty features:

Vance E. Drawdy, Shareholder, **Ogletree Deakins**, Greenville, S.C.

Stephen A. Riga, Esq., **Ogletree Deakins**, Indianapolis

Timothy G. Verrall, Shareholder, **Ogletree Deakins**, Houston

The audio portion of the conference may be accessed via the telephone or by using your computer's speakers. Please refer to the instructions emailed to registrants for additional information. If you have any questions, please contact **Customer Service at 1-800-926-7926 ext. 10**.

Tips for Optimal Quality

FOR LIVE EVENT ONLY

Sound Quality

If you are listening via your computer speakers, please note that the quality of your sound will vary depending on the speed and quality of your internet connection.

If the sound quality is not satisfactory, you may listen via the phone: dial **1-866-258-2056** and enter your PIN when prompted. Otherwise, please **send us a chat** or e-mail **sound@straffordpub.com** immediately so we can address the problem.

If you dialed in and have any difficulties during the call, press *0 for assistance.

Viewing Quality

To maximize your screen, press the F11 key on your keyboard. To exit full screen, press the F11 key again.

Continuing Education Credits

FOR LIVE EVENT ONLY

For CLE purposes, please let us know how many people are listening at your location by completing each of the following steps:

- In the chat box, type (1) your **company name** and (2) the **number of attendees at your location**
- Click the SEND button beside the box

If you have purchased Strafford CLE processing services, you must confirm your participation by completing and submitting an Official Record of Attendance (CLE Form).

You may obtain your CLE form by going to the program page and selecting the appropriate form in the PROGRAM MATERIALS box at the top right corner.

If you'd like to purchase CLE credit processing, it is available for a fee. For additional information about CLE credit processing, go to our website or call us at 1-800-926-7926 ext. 35.

Program Materials

FOR LIVE EVENT ONLY

If you have not printed the conference materials for this program, please complete the following steps:

- Click on the ^ symbol next to “Conference Materials” in the middle of the left-hand column on your screen.
- Click on the tab labeled “Handouts” that appears, and there you will see a PDF of the slides for today's program.
- Double click on the PDF and a separate page will open.
- Print the slides by clicking on the printer icon.

Data Breaches in ERISA Benefit Plans: Prevention and Response

Vance E. Drawdy (Greenville), Timothy G. Verrall (Houston), Stephen A. Riga (Indianapolis)

Best Lawyers® BEST LAW FIRMS U.S.News & WORLD REPORT EMPLOYEE BENEFITS (ERISA) LAW – TIER 1 NATIONAL 2015

Ogletree Deakins

ogletreedeakins.com

Overview

- The Background: Who, what, when, and how?
- The Legal Framework
- Assessing the Anthem Breach
- Key Take-Aways

The Anthem Data Breach: A Case Study

The Breach

- February 5, 2015: Anthem Blue Cross/Blue Shield announces that its servers were accessed by an unauthorized party
  - Breach began on December 10, 2014
  - Discovered on January 29, 2015
- Approximately 80 million Anthem customers were affected
  - All insurance lines were affected – not just health

What Happened?

- Breach was apparently a purposeful attack
- Attacker was able to gain entry to internal database using valid administrator credentials
- Anthem response:
  - Involve law enforcement, including the FBI
  - Retain forensic IT consultant to assess scope of breach
  - Communicate with state/federal regulators, other Blue Cross Blue Shield insurers, members, employers
  - Credit monitoring services

What Information Was Included?

- Information at issue included:
  - Names
  - Member ID numbers
  - Dates of birth
  - Social Security numbers
  - Addresses, phone numbers
  - Email addresses
  - Employment information, including income data
- Anthem reported that no financial or health information was compromised
  - How is HIPAA implicated then?

Initial Responses

- State regulators sent a letter demanding action February 10, 2015
- Class action litigation filed almost immediately after announcement
- Phishing attempts on many affected individuals
- Many questions from employers with current or former relationship with Anthem
- Spotlight on data security with Executive Order issued on February 13, 2015

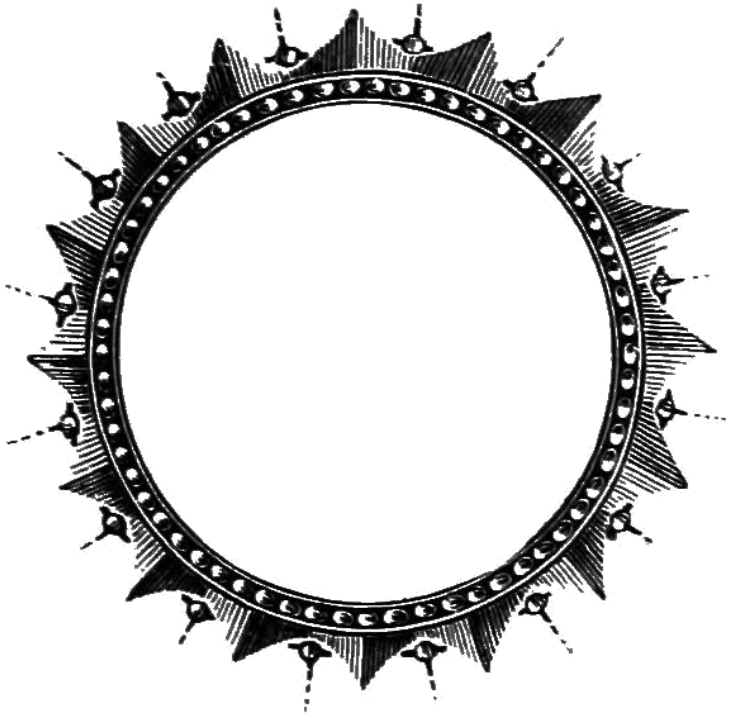
Notices Issued

- Notices to individuals sent over several weeks, starting the week of February 23rd
  - Sending approximately 2.5 million notices per day
  - Complaints continue about the speed of Anthem's response
- Some employers receiving census information
  - Data often more detailed than the notice sent to covered individuals
  - Includes granular information about data at issue

Premera: Another Shoe Drops

- March 17, 2015: Premera Blue Cross announced another major breach in the health insurance industry
  - Breach began on May 5, 2014
  - Discovered on January 29, 2015
- Approximately 11 million affected individuals
- Data includes identifying information, like Anthem breach, but also
  - Bank account information
  - Claims information, including clinical information

Responding to Data Breaches: *The Legal Framework*



What Laws Are Implicated?

- The security of personally-identifiable information is regulated at the Federal and state level
  - Our focus today is on HIPAA/HITECH and state breach notification requirements
  - An array of Federal financial privacy rules may be implicated in other breach situations
- HIPAA/HITECH breach notification requirements apply to protected health information
- State-level breach requirements generally apply to personally-identifiable financial, medical, and similar information
  - An identifier + account number, SSN, etc.
  - Focus is on information that facilitates ID theft

HIPAA & HITECH

- HIPAA regulates the use/disclosure of PHI
  - Individually-identifiable information involving medical care, medical condition, or payment for medical care
  - Broadly construed by DHHS
- HIPAA applies to covered entities—
  - Employer group health plans
  - Health insurance issuers
  - Many healthcare providers
  - Healthcare clearinghouses
- HIPAA also applies to business associates hired by covered entities
  - Vendors hired to provide support services with the use/disclosure of PHI
  - TPAs, brokers, consultants, etc.

HIPAA & HITECH (cont.)

- Employers (plan sponsors) are not directly subject to HIPAA but are effectively responsible for compliance on behalf of their health plans – which are covered
- Extent of employer responsibilities depends on plan design:
  - Fully-insured plan: limited employer responsibilities
  - Self-funded plan: significant employer responsibilities
- Under HITECH amendments (2009), vendors are regulated directly by many HIPAA requirements
  - Data security requirements apply
  - Privacy requirements apply by contract
- HITECH also created data breach rules

HIPAA Data Breach Rules

- Created HITECH Amendments in 2009
  - Final regulations issued in 2013
  - Supplements state breach notice requirements
- Any use/disclosure of PHI that is not permitted by HIPAA is presumptively a breach
  - Low probably of compromise?
  - Risk of harm standard no longer applies
  - Some limited exceptions apply
- A data breach triggers notice obligations and requires appropriate mitigation

HIPAA Data Breach Rules (cont.)

- The covered entity is responsible by default for assessing the situation and determining whether or not a breach as occurred
  - The relevant covered entity may be the group health plan or the insurer
  - Employer's role will depend on the type of plan at issue
- For insured plans, the insurer will typically be responsible for breach assessment and notification
- For self-funded plans, breach assessment and notification responsibilities can be – and often are – delegated to the business associate involved

HIPAA Data Breach Rules (cont.)

- Under HIPAA, notices to be provided without unreasonable delay and in no event more than 60 days after discovery of a breach
- If breach at BA level, BA to report to covered entity without unreasonable delay and within 60 days of discovery, subject to terms of BA agreement
  - Is the BA an “agent” of the plan?

HIPAA Data Breach Rules (cont.)

- Notification must be provided to—
  - Affected individuals
  - DHHS (immediately or annually)
  - Media outlets (large breaches)
- HIPAA and state notices can be consolidated
  - Watch for idiosyncratic state requirements

HIPAA Data Breach Rules (cont.)

- Notification must include:
  - Date of discovery
  - Date of breach (if known)
  - A description of the breach (but avoid too much detail)
  - Information about how the individual can protect him/herself
  - A description of any mitigation or corrective action being taken
  - Contact information
- Deliver notices by first class mail

State Data Breach Laws

- Forty-seven states have adopted some form of breach notification requirement
- Laws focus on unauthorized use or disclosure of personally-identifiable information
  - Medical information is usually included, but laws are broader
- A breach may trigger—
  - Notice obligations to affected individuals
  - Notice obligation to designated state officials (AG, Insurance Commissioner)
  - Reporting to consumer credit agencies
  - Mitigation (e.g., credit monitoring services)
- State laws that are stricter than HIPAA will control if there is overlap

ERISA

- ERISA regulates operation of private-sector employee benefit plans
  - Group health plans are HIPAA covered entities
- Plan fiduciaries are obligated to:
  - Act prudently
  - Follow the plan terms
- HIPAA provisions may be incorporated into group health plans
  - Fully-insured: Less likely, but possible
  - Self-funded: Very likely to include HIPAA provisions
- A data breach could trigger fiduciary conduct concerns

Assessing a Third Party Breach

First Steps

- What is your relationship to the company with the breach?
  - Policyholder – insured health plan
  - Business partner – self-funded health plan
  - Policyholder – insured non-health plan (e.g., life/AD&D)
- Assess responsibilities based on company's role
  - Insured health plan – Insurer is primary
  - Self-funded health plan – Plan is primary; check the contract
  - Insured non-health plan – Insurer is primary; HIPAA not implicated

Insured Plans – Action Items

- Insurer bears primary responsibility for breach response, state and Federal
  - Anthem proceeded on this basis
- Communicate early and often
  - Confirm who was affected
  - Ensure employees are receiving “official” communications
  - Consider supplementing communications
- Seek input on notification
- Supplement mitigation (e.g., additional identity theft protections)

Self-Funded Plans – Action Items

- Plan has primary responsibility by default
  - Assess ASO, BA, and other agreements with the company who experienced the breach to determine whether breach notice responsibility has been assumed by the other party
  - Consult plan's HIPAA policies and procedures
- If company has more limited role:
  - Document breach assessment per HIPAA policies
  - Determine who was affected
  - Determine appropriate mitigation
  - Prepare and distribute required notices
  - Consult service agreements to determine responsibilities

All Plans – Action Items

- Be proactive in communications with third parties to ensure access to latest information
  - Much remains to be learned about the breach
- Coordinate response to ensure both Federal and state notice requirements are satisfied in a timely and accurate manner
- Communicate with affected employees to satisfy ERISA responsibilities and to avoid misinformation
- Pursue information from the company about corrective actions – avoid a repeat

Employee Communications

- Communications from a third party may be official, but are not tailored to your workforce
  - Employers may wish to supplement official communications, even if they are not mainly responsible for breach response
- Things to consider:
  - Avoid hasty, ad hoc communications
  - Avoid conflicts with other communications
  - Direct employees to official communications as available
- Monitor communications and anticipate problems before they arise

So, What Now?

An Ounce of Prevention…

- Employers and their plans are poorly positioned to actively monitor security measures of insurers and other third parties that work with their plans
- Carefully review security provisions in contracts, insurance policies
- Ask questions now about the precautions insurers and service providers are taking to address the risks
- Assess your own policies and procedures and fill the gaps you identify in your own security efforts

…Is Worth a Pound of Cure

- Anthem and Premera have been the victims recently, but expect more breaches
- Determine your relationship with any company that announces a breach
- Assess HIPAA policies regarding data breach response
- Assess contractual responsibilities for breach analysis and response

A Pound of Cure (cont.)

- Consider state breach notification responsibilities and ERISA fiduciary conduct standards
- Communicate with your employees and the insurer or third party
- Explore additional protections for employees, depending on the company's mitigation proposals

Questions?

Vance E. Drawdy
vance.drawdy@ogletreedeakins.com

Stephen A. Riga
stephen.riga@ogletreedeakins.com

Timothy G. Verrall
timothy.verrall@ogletreedeakins.com