KRIEG|DEVAULT

GROUP HEALTH PLANS: 2010 WINTER COMPLIANCE UPDATE

Indiana Benefits Conference
January 19, 2010
Presented by:
Catherine (Katy) Stowers, Esq.

HIPAA Privacy and Security Changes Under the HITECH Act

KRIEG|DEVAULT

HIPAA 101: HIPAA Compliance Prior to HITECH

- Health Plans, Health Care providers and Health Care Clearinghouses = Covered Entities (CEs).
- HIPAA applied directly and only to CEs.
- HIPAA Privacy Rules required CEs to have (among other things) HIPAA Privacy Policies and Procedures, Notices of Privacy Practices and Training of employees.
- Self-Funded Plans Required to fully comply with HIPAA.
- Fully-Insured Health Plans had a pass on much of HIPAA Privacy requirements, and limited security obligations because of limited ePHI access.

KRIEG|DEVAULT

HIPAA 101: HIPAA Compliance Prior to HITECH

- Business Associates (BAs) of CEs ONLY obligated to comply with HIPAA as required in Business Associate Agreements (BAAs).
- Informal Compliance Assistance provided by CMS and OCR; enforcement was not aggressive and health plan HIPAA audits were uncommon.
- No Private Right of Action.

KRIEG|DEVAULT

HIPAA Changes in ARRA

- The American Recovery and Reinvestment Act of 2009 (ARRA) was signed into law on February 17, 2009.
  - The Health Information Technology for Economic and Clinical Health Act ("HITECH Act") amended HIPAA relating to health records, health information exchanges and data breaches
  - Generally effective beginning February 17, 2010

KRIEG|DEVAULT

Applicability of HIPAA Privacy & Security Rules to Business Associates

- **Effective February 17, 2010**, Business Associates (BAs) are required to directly comply with the HIPAA Security Rules in the same manner as Covered Entities. BAs are also required to comply with the HIPAA Privacy Rules as required under BA agreement.
- BAs ***directly subject to*** HIPAA's civil and criminal penalties for violations of Security Rule or BA agreement provisions.

KRIEG|DEVAULT

Action Required: BAs need to take required steps to comply with HIPAA Privacy & Security Rule provisions.

Privacy Action Steps

- Review existing BA agreements to determine if new ARRA requirements are incorporated into existing agreements, and amend if necessary
- BAs must comply with all HIPAA Privacy Rule requirements extended to the BA through the terms of the BA agreement (including adopting and implementing HIPAA policies and procedures)
- Penalties & sanctions apply directly to BAs for violations

KRIEG|DEVAULT

Action Required: BAs need to take required steps to comply with HIPAA Privacy & Security Rule provisions

Security Action Steps : (If not already in place)

- HIPAA's Security Rule applies to protected health information in electronic form ("ePHI")
- Appoint a security official to oversee security responsibilities
- Adopt written policies and procedures to demonstrate compliance with security provisions
- Review existing BA agreements to ensure incorporation of new ARRA requirements, and amend if necessary
- Adopt administrative, physical and technical safeguards for e-PHI

KRIEG|DEVAULT

Privacy and Security Policies and Procedures

Policies should address the following:

- Administrative Compliance Measures (e.g. training, appointment of privacy/security official, complaint procedure, record maintenance)
- Creation and Maintenance of PHI (e.g. defining PHI, establishing storage and retention policies)

KRIEG|DEVAULT

Privacy and Security Policies and Procedures

- Permitted Uses and Disclosures (e.g. treatment, payment, health care operations ("TPO"), participant disclosures, legally required disclosures, disclosures pursuant to authorization)
- Identification and Protection of Participant Rights (e.g. right to privacy notice, to restrict use and access of PHI, to receive accounting of unauthorized disclosures)

KRIEG|DEVAULT

Privacy and Security Policies and Procedures

- Internal Safeguards for PHI (e.g. access controls, firewalls, encryption, password protection, marketing and sale restrictions)
- Complaint and Sanction Procedures for Violations of Policies
- Process for Identifying and Addressing Administrative, Technical and Physical Safeguards Required by Security Rule

KRIEG|DEVAULT

CEs Obligated to Notify Individuals and Others of Breach Involving PHI: The Breach Notification Regulations

- CEs are required to notify individuals whose "unsecured" PHI has been accessed, acquired or disclosed as a result of a "breach." BAs are still obligated to notify CEs of any such incidents, but language has been added that requires notice to include "identification of each individual" whose PHI was the subject of the breach. BAs must notify CEs as soon as possible, but in no event later than 60 days after of discovery of the breach. Interim Regulations make new "Breach Notification" requirements effective as of September 23, 2009 (sanctions applicable beginning February 22, 2010).

KRIEG|DEVAULT

Protected Health Info

A Breach Involving PHI

New regulations define "Breach" as the ***unauthorized*** acquisition, access, use or disclosure of PHI in a manner that compromises the security or privacy of the PHI. Security or privacy is compromised if the use or disclosure "poses a significant risk of financial, reputational or other harm to the individual."

If an unauthorized use or disclosure is discovered, the CE or BA must perform a risk assessment to determine if the use or disclosure poses a significant risk of harm, and thus whether a Breach has occurred requiring notification.

KRIEG|DEVAULT℠

Secured PHI Exempted from Breach Notification

- PHI is considered secured when it has been encrypted (rendered indecipherable) or it has been destroyed
- PHI in a Limited Data Set is ***NOT*** considered secured unless all identifiers ***plus*** zip codes and dates of birth are removed
- Encryption is not required, but is a safe harbor from breach notification rules
  - May transmit ePHI via password-protected e-mails, or store through use of firewalls, but breach notification rules will apply to unauthorized uses and disclosures

KRIEG|DEVAULT℠

Required Action Steps in the Event of a Breach

Discovery of the Breach

- Breach is considered discovered as of the 1st day of the breach being known by the CE or BA, or when, by exercising reasonable diligence, it would have been discovered by the CE or BA.
- Knowledge of a breach by a workforce member or agent (BA) is attributed to the CE
- Time period begins to run upon knowledge of event occurring, even if it is unclear whether incident meets the regulatory definition of Breach.

KRIEG|DEVAULT℠

Required Action Steps in the Event of a Breach

- Determine if breach notification is required:
  - Did impermissible use or disclosure of Unsecured PHI occur?
  - If yes, conduct and document a risk assessment to determine whether the impermissible use or disclosure compromised the security or privacy of the PHI
    - Did it create a significant risk of financial, reputational or other harm to the individual? Subjective analysis.
    - If yes, notification to the affected individuals is required.

KRIEG|DEVAULT

Notification of Breach to Individuals

- Notification to individuals required without unreasonable delay, and no later than 60 calendar days after incident is discovered.
- Breach notice should contain:
  - A brief description of the incident
  - A description of the types of unsecured PHI involved in the breach (but not the actual PHI)
  - Steps to take to protect individuals from potential harm resulting from the breach
  - Brief description of what the CE is doing to investigate, mitigate, and protect against further breaches
  - Contact information, which must include: toll-free number, an email address, Website, or postal address.

KRIEG|DEVAULT

Notification to Media Outlets and Secretary of HHS

- If CE ***does not have contact information for 10 or more affected individuals***, then CE must post a conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside.
- If ***more than 500 residents of a state***, CE must notify prominent media outlets of the breach. (This is in addition to the individual notices mentioned above).
- If ***more than 500 individuals' PHI involved***, then the CE must notify the Secretary of HHS of the breach.
- If PHI of less than 500 individuals involved, then CE may either notify HHS of the breach or may maintain a log of breaches that occur during the year, but must submit to HHS within 60 days after the end of the calendar year. ***Breach logs must be maintained for 6 years.***

KRIEG|DEVAULT

Heightened Civil Enforcement of HIPAA Privacy & Security Rules

- Civil penalties increased and HHS is ***required*** to investigate any complaints that may have resulted from "willful neglect" by a CE or a BA.
- Interim Final Regulations on Penalties were effective on November 30, 2009, and apply to violations on or after February 18, 2010

KRIEG|DEVAULT

New Penalty Structure under Interim Final Regulations

- If CE or BA unaware or would not have known of the violation by exercising reasonable diligence, minimum civil penalty is $100 per HIPAA violation, with per-violation max of $50,000, and an overall limit of $1,500,000 for identical violations during calendar year.
- If violation due to reasonable cause and not willful neglect, minimum is $1,000 per violation, with per-violation maximum of $50,000, an overall $1,500,000 limit for identical violations per calendar year.
- If violation resulted from willful neglect but is corrected within 30 days of discovery, minimum is $10,000 per violation, with per-violation max of $50,000, and an overall $1,500,000 limit for identical violations per calendar year.
- If violation is due to willful neglect and not corrected, minimum is $50,000 per violation, and an overall $1,500,000 limit for identical violations per calendar year.

KRIEG|DEVAULT

Definitions from Interim Final Regulations on Penalties

- **Reasonable Cause**: circumstances that would make it unreasonable for the CE or BA to comply with the provision despite the exercise of ordinary care and diligence.
- **Reasonable Diligence**: the business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances.
- **Willful Neglect**: conscious, intentional failure or reckless indifference to the obligation to comply with the provision that was violated.

KRIEG|DEVAULT

Criminal Liability Under HIPAA Extends to Entities and Individuals

- Effective February 17, 2010, ***CEs, as well as BAs and other actors*** who obtain or disclose protected health information ("PHI") maintained by a CE without authorization, may also be criminally liable.

KRIEG|DEVAULT

Potential Causes of Action for Breach

- In addition to criminal and civil penalties the new law creates additional remedies:
  - State Attorneys General may bring action for injunctive relief or damages on behalf of state residents adversely affected by HIPAA violations
  - Individuals will be awarded a percentage of civil monetary penalties collected for violations

KRIEG|DEVAULT

Additional HIPAA Rights and Obligations Impacted By HITECH

- "Minimum Necessary" disclosures restricted; regulations expected
- "Health Care Operations" definition will be modified to further restrict disclosures for TPO; regulations expected
- Increased restrictions on marketing and sale of PHI
- Changes made to individual rights –
  - Additional restrictions on disclosures to health plans (cash payments)
- Changes related to Electronic Health Records ("EHRs")
  - If EHRs used, CE must account for all uses and disclosures
  - Requires CEs to provide PHI electronically if EHRs used

KRIEG|DEVAULT

COBRA Subsidy Extension under 2010 Department of Defense Appropriations Act

KRIEG|DEVAULT

Original ARRA Subsidy Provisions

- ARRA implemented 65% COBRA premium subsidy for "assistance eligible individuals" ("AEIs") – plan participants involuntarily terminated between 9/1/08 and 12/31/09
- AEIs eligible for COBRA subsidy for 9 months
- Employers recapture subsidy through payroll tax credit

KRIEG|DEVAULT

Appropriations Act Modifications to ARRA

- Extends AEI qualification period to involuntary terminations occurring on or before February 28, 2010
- Extends the COBRA subsidy eligibility period from 9 months to 15 months
- Creates additional notice requirements

KRIEG|DEVAULT

Notice Requirements

- Plan administrators (or COBRA administrators) must provide "premium assistance extension notice" to:
  - AEIs receiving premium assistance as of 10/31/09;
  - Any qualified beneficiary (including AEIs) who received general COBRA notice after 10/31/09 without updated subsidy extension information included.
- General notice must be updated to include subsidy extension information for all COBRA qualified beneficiaries.
- Extension Notices must be issued by February 17, 2010

KRIEG|DEVAULT

Special Coverage Requirements

- If AEI exhausted subsidy period prior to enactment of extension, and failed to pay COBRA premium in the subsequent month, group health plan must allow retroactive reinstatement of coverage.
- AEI must remit retroactive premium payments by **the later of** February 17, 2010 or 30 days after notice of premium extension provided to AEI
- A participant may qualify as an AEI if involuntary termination occurs on or before 2/28/10, even if plan coverage not lost until after 2/28.

KRIEG|DEVAULT

Group Health Plan Excise Tax Reporting Requirements

KRIEG|DEVAULT

New Obligation to Report

- Final Regulations issued September 8, 2009 require employers who sponsor group health plans (and potentially insurance companies, TPAs and HMOs) to report excise tax due under IRC Sections 4980B, 4980D, 4980E, and 4980G.
- Excise Tax reported on Form 8928
- Effective for violations occurring on or after January 1, 2010

KRIEG|DEVAULT

Violations Subject to Reporting

- §4980B – violations of COBRA's notice, coverage and premium provisions
- §4980D – violations of HIPAA portability and nondiscrimination provisions, Michelle's Law, Mental Health Parity Act, Newborns and Mothers Health Protection Act, Women's Health and Cancer Rights Act, Genetic Information Nondiscrimination Act, guaranteed renewability requirements for multiemployer and multiple employer plans
- §4980E – violations of Archer MSA comparability rules
- §4980G – violations of HSA comparability rules

KRIEG|DEVAULT

Due Dates for Filing Form 8928

- Violations of § 4980B or §4980D (COBRA, HIPAA and other health plan mandates)
  - Employers (and insurers/TPAs if responsible for administering health plan benefits):
    - on or before the due date of the corporate tax return applicable to the noncompliance period, without regard to extensions.
  - Multiemployer and multiple employer health plans:
    - on or before the last day of the seventh month following the plan year in which the violations occurred.

KRIEG|DEVAULT

Due Dates for Filing Form 8928

- Violations of § 4980E or § 4980G (comparability rules)
  - Employers must file on or before the 15th day of the 4th month following the calendar year in which the violations occurred.

KRIEG|DEVAULT

Unanswered Questions

- Regulations require affirmative reporting of violations on Form 8928 and payment of excise taxes without "assessment" or "notice and demand." Filers must voluntarily report.
- No excise tax is due for group health plan requirements where compliance failures are unknown despite reasonable diligence, and where the failure is due to reasonable cause, corrected in a timely manner, and affected individuals are "made whole."
  - Who makes this determination?
  - What if IRS later discovers error and disagrees?
  - What are the penalties for nonfiling?
    - $2500 if filing is after examination; $15,000 if violation is not "de minimus"
    - Interest and penalties?

KRIEG|DEVAULT

QUESTIONS???

CONTACT INFORMATION

- **Katy Stowers**
  cstowers@kdlegal.com
- (317) 238-6257

24967871v1

KRIEG|DEVAULT