BakerHostetler

Be Careful What You Wish For: The Final Rule Is Out

Theodore J. Kobus III
tkobus@bakerlaw.com
@tedkobus
212.271.1504

Lynn Sessions
lsessions@bakerlaw.com
@lynnsessions
713.646.1352

Toll Free 24-Hour Data Breach Hotline **855.217.5204**

Blog: www.dataprivacymonitor.com

Theodore J. Kobus III

BakerHostetler

Ted Kobus is National Co-Leader of the Privacy and Data Protection Team.

Ted advises clients, trade groups and organizations regarding data security and privacy risk management, breaches, response strategies, litigation and regulatory actions affecting organizations. He has counseled clients involved in over 400 breaches, including significant breaches implicating state and federal laws, international laws and other regulations and requirements: HITECH, the Massachusetts Data Privacy Law, California privacy laws (including the California Department of Public Health Law), Connecticut Insurance Department regulations, Puerto Rico's Citizen Information on Data Banks Security Act, Mexico's Data Protection Law, Canada's data privacy requirements and PCI/CISP requirements. He has dealt with Offices of Attorneys General, state insurance departments, Office of Civil Rights (OCR)/Health and Human Services (HHS), Secret Service, FBI and local police and forensics professionals as part of their handling of data breaches.

Lynn Sessions

BakerHostetler

Lynn Sessions focuses her practice on providing legal services to healthcare industry clients, including hospitals, integrated delivery systems, healthcare providers, and academic medical centers. Using her prior in-house experience at Texas Children's Hospital, Lynn represents and provides legal counsel to clients on a variety of privacy and data security matters from an in-house counsel and client perspective. Lynn works with clients to ensure they are in compliance with HIPAA/HITECH regulations, develops proactive compliance programs, provides counsel in response to a privacy or data breach, and works with clients to ensure the effective development of preventative data privacy and security measures.

Lynn has worked with clients where multiple parties in various states were involved in high stake data privacy security breaches. She is experienced in applying federal HIPAA/HITECH regulations and specific state privacy and breach statutes and the OCR and other regulatory investigations that follow. Lynn has handled internal investigations on a large and small scale. These investigations are focused on protecting health care providers and their customers from privacy and data breaches, and fraud and identity theft. Ms. Sessions has also worked with clients to develop preventative data privacy and security strategies to avoid potential security breaches, including development of policies and procedures, breach response teams and training programs.

OCR Resolution Agreements

BakerHostetler

- Providence Health & Services ($100K)
- CVS Pharmacy ($2.25M)
- Rite-Aid ($1M)
- Management Services Organization of Washington ($35K)
- Cignet ($4.3M)
- Massachusetts General Hospital ($1M)
- UCLA Health Services ($865K)
- Blue Cross Blue Shield of Tennessee ($1.5M)
- Alaska Medicaid ($1.7M)
- Phoenix Cardiac Surgery, P.C. ($100K)
- Massachusetts Eye and Ear Infirmary ($1.5M)
- Hospice of North Idaho ($50K)

What Has OCR Said About Enforcement?

BakerHostetler

"This final omnibus rule marks the most sweeping changes to the HIPAA Privacy and Security Rules since they were first implemented. These changes not only greatly enhance a patient's privacy rights and protections, ***but also strengthen the ability of my office to vigorously enforce the HIPAA privacy and security protections***, regardless of whether the information is being held by a health plan, a health care provider, or one of their business associates."

Director OCR

Leon Rodriguez

Business Associates Are Now Directly Liable

BakerHostetler

- §160.402: Basis for a Civil Monetary Penalty.
- §160.402(c)(2): A business associate is liable, in accordance with the Federal common law of agency, for a civil money penalty for a violation based on the act or omission of any agent of the business associate, including a workforce member or subcontractor, acting within the scope of the agency.
- §160.103: A business associate includes "[a] subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate."

Calculation of Civil Monetary Penalties (CMPs)

BakerHostetler

- §160.408 Factors considered in determining the amount of a civil money penalty.
- The Secretary MUST consider a list of mitigating or aggravating factors.
  - The nature and extent of the violation (number of individuals affected, time period during which the violation occurred, the
    - number of individuals affected.
    - time period during which violation occurred.
    - the nature and extent of resulting harm (physical harm, reputational harm, or financial harm).
    - whether the violation hindered ability to obtain health care (“facilitated” removed).

Calculation of Civil Monetary Penalties (CMPs)

BakerHostetler

- The Secretary MUST consider a list of mitigating or aggravating factors
  - The history of prior compliance and attempts to correct indications of noncompliance.
  - Response to technical assistance from the Secretary.
  - Response to prior complaints.
  - Financial condition of CE or BA.
  - Size of the BA or CE.
  - Such other matters as justice may require.

Assurances to Safeguard Information

BakerHostetler

- Covered Entities (CEs) must receive assurances from Business Associates (BAs).
- CEs do not need to receive assurances from Sub-Bas.
- BAs need to receive assurances from SubBAs.
- Sub-Business Associate Agreements (subBAA's) required.
- Violation if CE/BA knows of a pattern of activity or practice of the BA/subBAA that constituted a material breach or violation of the BA's/subBA's obligation under the contract or other arrangement, unless the CE/BA took reasonable steps to cure the breach or end the violation, and, if such steps were unsuccessful terminated the contract or arrangement if feasible.

Disclosures by BAs

BakerHostetler

- BAs are limited to the scope of their contract with the CE.
- BAs are not engaged in healthcare operations, so there is no TPO exception.
- Focus on the contract with the CE.
- Minimum Necessary applies.

Minimum Necessary

BakerHostetler

What is a Breach?

BakerHostetler

- Baseline Definition of a Breach remains unchanged.
- §164.402: Breach means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information.

Interim Final Rule Breach Definition

BakerHostetler

- Compromise.
- Poses a significant risk of financial, reputational, or other harm.
- Focus was on the harm to the individual.

Definition of Breach in Final Rule

BakerHostetler

- An acquisition, access, use, or disclosure of protected health information in a manner not permitted . . . is ***presumed*** to be a breach.
- Unless, the CE or BA can demonstrate that there is a low probability that the PHI has been compromised based on a risk assessment.
- Compromise is not defined.

Definition of Breach in Final Rule

BakerHostetler

Risk Assessment

- Documented
- Based on at least 4 factors
  - The nature and extent of the PHI.
  - The unauthorized person involved.
  - Whether the PHI was actually acquired or viewed.
  - Extent to which any risk has been mitigated.

Reporting/Notification Clarifications

BakerHostetler

- Notification, in situations where the use or disclosure is so inconsequential, is not warranted because it may cause the individual unnecessary anxiety or even eventual apathy if notifications of these types of incidents are sent routinely.
- Substitute notice or media notice may at times occur after the 60-day period depending on circumstances.
- Breaches under 500 must be reported no later than 60 days after the calendar year in which they were discovered, not when they occurred.
- Notification to the Secretary must occur contemporaneously with notice to individuals for breaches over 500.

A Few Things Remain the Same

BakerHostetler

- Timeliness and content of notification.
- A CE retains the ultimate obligation for proper notification.
- Notification by the BA can be delegated.
- Media notification and notification to HHS has not changed.
- Law enforcement delays remain available.
- There are no changes to the circumstances permitting preemption of state law of HITECH.

What Can You Do to Prepare?

BakerHostetler

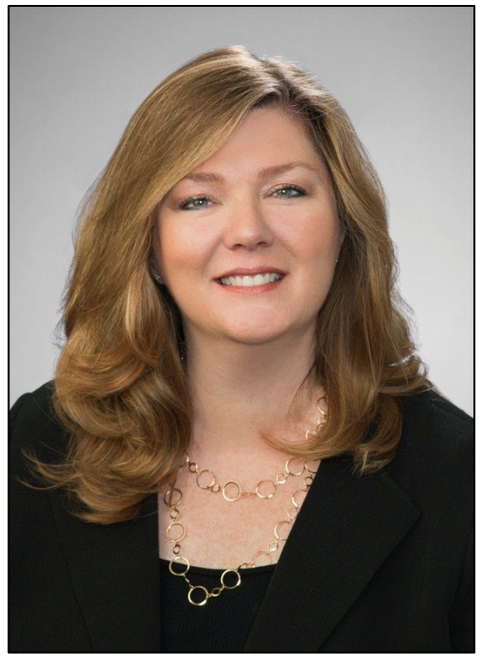
- Update your Incident Response Plan (IRP)
- Update your Policies & Procedures
- Breach Analysis Forms
- Education & Awareness
- Vendor Lists & Contracts
- Risk Assessments & Risk Management Plans
- Privacy Counsel
- Cyber Insurance
- Forensics

Additional Questions?

BakerHostetler

- Please contact

Ted Kobus
212.271.1504
tkobus@bakerlaw.com



Lynn Sessions
713.646.1352
lsessions@bakerlaw.com

Toll Free 24-Hour Data Breach Hotline **855.217.5204**

BakerHostetler

Chicago
Cincinnati
Cleveland
Columbus
Costa Mesa
Denver
Houston
Los Angeles
New York
Orlando
Washington, DC

www.bakerlaw.com