**Global Data Privacy and Security Team**

Bryan Cave's Global Data Privacy and Security Team works with data security and risk assessment issues to routinely help clients before a breach happens analyze and improve upon their ability to respond to, and minimize the liability from, a breach if (or when) one occurs.

For more Information Contact:

**David A. Zetoony**
Partner
david.zetoony@bryancave.com
1155 F Street, N.W.
Washington, D.C. 20004
T: 202 508 6000

One Boulder Plaza
1801 13th Street, Suite 300
Boulder, CO 80302-5386
T: 1 303 444 5955

**Sheryl Feutz-Harter**
Counsel
sheryl.feutzharter@bryancave.com
One Kansas City Place
1200 Main Street, Suite 3800
Kansas City, MO 64105-2122
1 816 374 3245

To join Bryan Cave's data privacy and security distribution list visit Bryan Cave Data Matters.

BRYAN CAVE

# Business Associates At A Glance: Responsibilities And Liabilities

The Health Information Technology for Economic and Clinical Health ("HITECH") Act modified the Health Insurance Portability and Accountability Act ("HIPAA") by expanding the definition of Business Associates ("BA") and their responsibilities and liabilities. A BA includes:

- Health Information Organizations
- E-Prescribing Gateways
- Persons/entities that for, or on behalf of, a Covered Entity:
  - Create or receive PHI
  - Maintain or store PHI even if they do not or can not access the PHI
  - Offer personal health records
  - Provide data transmission services if they routinely access the PHI

Pursuant to HITECH and HIPAA, BAs are required to do the following:

| | | | |
|---|---|---|---|
| **Designate Security Officer** | **Perform Security Risk Assessment** | **Implement Administrative, Physical, and Technical Safeguards** | **Identify and Report Breaches and Security Incidents** |
| **Develop Polices for HIPAA/HITECH Compliance Program** | **Impose Disciplinary Actions for HIPAA/ HITECH Violations** | **Have Business Associate Agreements with Subcontractors** | **Maintain Documentation 6 Years** |

The Federal Office for Civil Rights ("OCR") enforces HIPAA and HITECH. BAs are under great scrutiny from the OCR as BAs have been identified as one of the OCR's top three enforcement priorities in 2016. Under HIPAA and HITECH, BAs are directly liable for compliance and subject to these monetary penalties:

| Violation Category | Each Violation | Maximum Penalty per Identical Provision Violated in Calendar Year |
|---|---|---|
| Did Not Know | $100 - $50,000 | $1,500,000 |
| Reasonable Cause | $1000 - $50,000 | $1,500,000 |
| Willful Neglect – Corrected | $10,000 - $50,000 | $1,500,000 |
| Willful Neglect – Not Corrected | $50,000 | $1,500,000 |

## Key Considerations for BAs:

- ☑ Determine if you are a BA
- ☑ Designate person to oversee a HIPAA/HITECH Compliance Program
- ☑ Identify high risks, e.g., mobile devices, emails, texting, medical devices
- ☑ Respond timely and effectively to breaches and security incidents
- ☑ Monitor, audit, and update privacy and security on ongoing basis
- ☑ Know the terms of Business Associate Agreements
- ☑ Prepare contingency/disaster plan
- ☑ Maintain adequate cyber insurance