

COMPLIANCE, RISK & RESILIENCE:

HIPAA COMPLIANCE & BUSINESS ASSOCIATES

Healthcare-covered entities are not only vulnerable to Health Insurance Portability and Accountability Act of 1996 (HIPAA) challenges from their own operations, but can also be potentially harmed by weaknesses in the compliance programs of their business associates and vendors.

Business associates can create negative financial, legal, and reputational consequences by their actions or inactions such as dumping un-shredded hospital records, marketing electronic health records software that failed a Meaningful Use audit, and running unencrypted server farms.

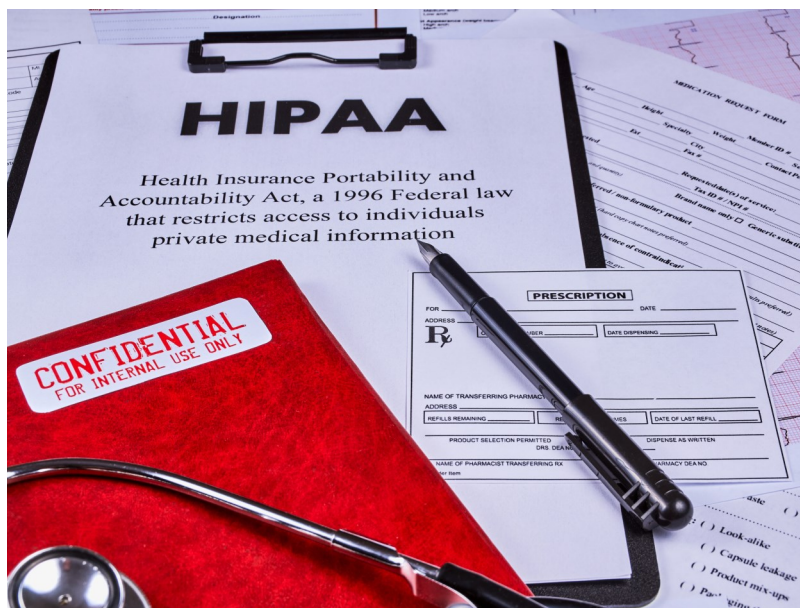
Covered entities have a fundamental incentive to better understand and manage their cyber-relationships with third parties, both operationally and through business associate agreements that robustly define responsibility and limit exposure.

The B. Riley Compliance, Risk and Resilience team understands all the stages of the business associate transaction that should be integrated by HIPAA-covered entities in their vendor risk management practices, including:

- RFP/RFQ/RFI procurement and evaluation documents, supported by periodically vetting supplier renewal
- Security and privacy risk assessments, as well as potential cyber risk implications imposed by business associates
- Business associate agreements, qualified service organization agreements, and service agreements

SERVICES

B. Riley helps clients understand the HIPAA and information security risks from the members of their supply chain using specialized vetting questionnaires and interviews, and providing response detail scoring and professional interpretation. We focus on the integration of client vendor processes, risk management, and business associate agreement language to help them minimize potential HIPAA vulnerabilities and exposures often created unknowingly by business associates and their subcontractors. Each stage of the business associate transaction requires appropriate processes, process language, and risk management visibility and oversight. In our assessments, we engage directly with clients or through outside legal counsel to ensure that clients can preserve the assertion of attorney-client privilege.



To help clients identify vendor risk, we use a basic questionnaire to guide business associate vetting during the procurement process, as well as a more detailed assessment to even more thoroughly identify potential vendor risk to the organization. We document response detail, analysis, scoring and interpretation around vendor:

- Qualifications and certifications
- Documentation, policies and procedures
- Primary Business Associate Agreements (BAAs) and agreements with business associate subcontractors
- Treatment of non-standard forms of ePHI
- Data location, data paths, storage, colocation and backup
- Status monitoring of workforce member disqualification and ineligible persons
- Training policy and documentation
- Incident, emergency and contingency plans
- Cyber supply chain risk management (C-SCRM)
- Risk analyses and prior event history
- Risk management and retention
- Data security
- Software settings and patches
- Administration and governance
- Facilities and physical security policies
- Paper files and waste security
- System development protocols

REPRESENTATIVE ENGAGEMENTS

University Medical School

Our team was retained on behalf of a university medical school to vet all business associates as part of a risk analysis. This resulted in the requirement for business associates to segregate university PHI, adopt and implement post-omnibus policies and procedures, consent to compliance audits and purchase of increased HIPAA-related insurance, encrypt their radiological files, and agree to tighter indemnification and audit rights in the BAA.

Multi-Location Community Hospital

Our team reviewed the data colocation vendor of a large, disperse community hospital. We found that the data center site was located within the same immediate geographical area and exposed to the same area hazards as the primary hospital data center. While the proximity supported the IT mission, copies of the data - and thus the back-up data center - should have been located out-of-area, to be fully viable and compliant.

THE B. RILEY DIFFERENCE

Our healthcare compliance professionals leverage their expertise as former chief compliance, privacy, information and, information security officers in the healthcare environment. We understand the vulnerability HIPAA- covered entities have from the performance or underperformance of their business associates. We know how best practices in vendor risk management extend into the information supply chains of our clients' business associates, why HIPAA compliance is only as good as the visibility clients have into their supply chain, why business associates can be among their greatest challenges, and just how vulnerable organizations can be to the obligations defined in their business associate agreements.

PRACTICE LEADER

Duane Lohn
dlohn@brileyfin.com
(602) 321-9818

Corey Gooch
cgooch@brileyfin.com
(312) 925-8550

ABOUT THE FIRM

ABOUT B. RILEY ADVISORY SERVICES

B. Riley Advisory Services provides specialty advisory services and solutions to complex business problems and board-level agenda items. Our team applies a unique mix of skill sets to address top-level, non-typical business challenges, such as developing compliance and risk systems for organizations, planning and executing a major acquisition or divestiture, pursuing a fraud investigation or corporate litigation, or managing through a business crisis or bankruptcy. In addition, we are a leading provider of valuation and appraisal services for asset-based lending applications.

Our team works with lenders, law firms, government entities, private equity sponsors and companies of all types. Our Advisory Services are a unique mix of Compliance, Risk & Resilience Services, Valuation and Appraisal Services, Restructuring and Turnaround Management, Operations Management Services, Forensic Accounting and Litigation Support and Transaction Support Services including Due Diligence and Quality of Earnings Reviews. B. Riley Advisory Services is a combination of the firms formerly known as GlassRatner Advisory & Capital Group and Great American Group.

ABOUT B. RILEY FINANCIAL (“B. RILEY”)

B. Riley Financial, Inc. (NASDAQ: RILY) companies provide tailored financial solutions to meet the strategic, operational, financial advisory and capital needs of its clients through a diverse range of collaborative and complementary business capabilities.

B. Riley's diverse suite of business capabilities goes beyond traditional financial service offerings. By leveraging cross-platform expertise and assets, our business units are uniquely positioned to provide full service, collaborative solutions at every stage of the business life cycle and in all market conditions.