

# Health Information Privacy and Security

The legislative and regulatory framework governing patient privacy has evolved and expanded dramatically since the passage of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). So, too, have the challenges of safeguarding patient data from increasingly sophisticated threats, all complicated by the proliferation of technologies designed to facilitate the exchange of and access to patient data. Hooper, Lundy & Bookman shepherds clients through the health information privacy and security landscape, combining our industry focus with technological acumen to protect patients and providers alike.

The foundation of our health information privacy and security practice is our comprehensive understanding of how the law and technology intersect in the day-to-day operations of providers, their business associates, suppliers, and others charged with protecting health information. HLB lawyers have been at the forefront of health care data security and privacy law for decades, possessing deep experience with the full spectrum of state, federal, and international laws and regulations impacting how the health care industry collects, manages, and protects patient data.

Clients in all sectors of the health care industry turn to HLB for our comprehensive counsel on data protection and patient privacy issues. Our clients include:

- Hospitals and hospital systems
- Physician groups
- Skilled nursing facilities and long-term care providers
- Mental health and substance abuse providers
- Pharmaceutical and device manufacturers
- Health information organizations (HIOs) and health information exchanges (HIEs)
- Medical app developers
- Pharmacies and pharmaceutical benefit managers
- Vendors, contractors, and other business associates

Our attorneys recognize that for clients working in health care, the foundational legal structures involving privacy and data protection, such as HIPAA, often only scratch the surface of their compliance obligations and concerns. Protecting providers, their patients, and their data requires an immersive understanding of a myriad of applicable laws, regulations, and regulatory guidance at the state, federal, and international levels, including:

- The HITECH Act of 2009
- The Family Educational Rights and Privacy Act (FERPA)
- Federal Trade Commission's (FTC) Health Breach Notification Rule for personal health records (PHRs)
- Children's Online Privacy Protection Act (COPPA)
- Telephone Consumer Protection Act (TCPA)
- Federal and state laws granting heightened protection to substance use disorder information, such as in 42 CFR part 2 ("Part 2"), behavioral health information, such as California's Lanterman-Petris-Short Act, and other equivalent laws
- The EU General Data Protection Regulation (GDPR) and other international privacy regulatory frameworks

HLB's full suite of health information privacy and security representation is both proactive and responsive, putting the structures in place to minimize the risks of breaches or non-compliance and acting quickly and decisively to address and

remediate any violations.

Below are examples of the services we offer to assist clients in navigating information privacy and security issues:

- Drafting, reviewing, and updating business associate agreements, patient authorizations, and notices of privacy practices for providers, suppliers, software developers and vendors, and case management and billing companies
- Developing HIPAA policies for “covered entities” and “business associates”
- Preparing limited data use and data license agreements
- Providing risk assessments under HIPAA's Breach Notification Rule and other federal and state data breach laws
- Counseling clients regarding security incidents, breaches, remediation, crisis management, reporting, and notification obligations
- Assisting with internal and government investigations
- Advising on privacy and security issues associated with transitioning to electronic medical record systems
- Providing HIPAA compliance training for employees
- Counseling on state data privacy and security laws, HIPAA preemption issues, and data exchange issues associated with health information exchanges, interoperability requirements, and data licensing agreements