Health Care Data Privacy and Security Fundamentals

BY CALVIN B. MARSHALL, JR.
Attorney, Chambliss, Bahner & Stophel, P.C.

As the "internet of things" continues to evolve, as data becomes ever more valuable in today's world, and as risks to data continue to proliferate, the importance of data privacy and security continues to grow. This is particularly the case in health care, where the data involved is both sensitive and very valuable to patients, providers, health care vendors, and also to bad actors. Organizations directly or indirectly involved with health care or health care entities should consider the following privacy and security fundamentals:

› Know What Health Care Privacy and Security Regulations Apply to Your Organization (and Don't Assume You Are Exempt)

For businesses that are health care providers, the HIPAA/HITECH regulations create a variety of obligations with respect to the use and disclosure of patient information, patient rights with respect to their information, the implementation of safeguards, and notification to patients and others in the event of data breaches. However, providers should also not lose sight of potential obligations under other federal law, such as 42 C.F.R. Part 2 (Confidentiality of Substance Use Disorder Patient Records), and under state-specific laws pertaining to the privacy and security of patient information.

For vendors rendering services to health care providers, determining whether they are subject to health care data privacy and security regulations can be more challenging. For example, many types of organizations become "business associates" subject to HIPAA/HITECH when they provide services to health care providers (or to other vendors of services to health care providers) and gain some level of control over or ability to access patient information. **Law firms, accounting firms, and information technology (IT)-related businesses**, among others, can step into this world without realizing the legal obligations they are taking on. As a result, organizations should be alert to the potential application of health care privacy and security regulations when providing any services that are directly or indirectly connected to health care.

› Take Necessary Steps to Comply with Applicable Regulations and Safeguard Data

Organizations subject to HIPAA should be aware that HIPAA requires them to create and formally adopt written policies that address a variety of HIPAA compliance matters in detail. Moreover, these organizations are required to implement a number of specific safeguards and to regularly conduct and document analyses of the risks and vulnerabilities to the electronic patient information they hold.

Beyond regulatory obligations, organizations should carefully evaluate their risks—obtaining expert advice where needed—and ensure they have appropriate safeguards in place to protect patient and proprietary health care data. Safeguards can range from administrative safeguards, such as limiting employee access to data when not needed to perform job functions, to technical safeguards, such as web and e-mail filters, robust firewalls, and anti-virus programs.

It is also essential to take steps to prepare for data breaches and security incidents, which sometimes occur despite best efforts to prevent them. These steps should include, among others, implementation and testing of breach/incident response plans to promote recovery rather than making the situation worse, purchase and careful vetting of cyber risk insurance to cover incident-related costs, and implementation of full and incremental offsite data backups to avoid loss of data.

› Address the Human Element

Most importantly, because so many cyberattacks depend on employee mistakes (e.g. clicking on that e-mail link) for their success, organizations should understand that robust system safeguards will not protect them if they do not also train and equip their employees. Organizations should be vigilant in their efforts to train employees on what is required of them for security and compliance purposes and to prepare them for the security threats (such as e-mail phishing campaigns) that they will inevitably face in the workplace. In addition to formal training, sending frequent reminders to employees regarding common security threats or security threats experienced by the organization is important, as is testing employee preparedness, such as through quizzes and artificial e-mail phishing campaigns.

› Bottom Line: Be Informed and Be Prepared

Organizations of all types and sizes—whether startups, emerging businesses, established companies or nonprofits—should carefully consider whether health care privacy and security regulations apply to them, taking steps to comply with applicable regulations, safeguard data, and ensure that the organization and its staff are appropriately prepared to encounter and respond to threats. With each passing year, the importance of data privacy and security continues to increase—both in health care and in other industries.

Cal Marshall works with local, regional, and national clients on a variety of health care and business matters, including compliance with federal and state privacy and security laws, data breach response, health care contracting, corporate governance, telehealth, fraud and compliance matters, Medicare enrollment and payment issues, and compliance with state laws and regulations. Prior to law practice, Cal served as an aide to several members of the U.S. House of Representatives, working on health care policy and government oversight matters, among others. Cal writes and speaks on health care legal issues and has served in multiple leadership roles within the American Bar Association's Health Law Section.