Six Ways for Data-Driven Medical Device Companies to Implement Effective Privacy and Security Measures

Kevin Coy and Andrew B. Flake

The increasing amounts of health information being generated, stored and collected have heightened the special risks medical device manufacturers have long faced. In addition to the nexus to patient health and safety, if a manufacturer does not address data privacy and security, it could face a wide range of regulatory consequences from multiple agencies. Hacks are a major risk, as is intellectual property theft. So what should a medical device manufacturer take into account when it comes to privacy and security safeguards? This article offers some best practices and insights for the medical device manufacture who is handling health information.

1. **Begin from day one.** Privacy and security should be incorporated from the outset — what FTC has referred to as privacy and security by design. Addressing privacy and security should begin from the first design conversations around a connected medical device or mobile application. What constitutes appropriate privacy and security controls will depend on a number of factors, including the kind of data being collected and used; the sensitivity of that information; what the purpose of the device or application is; and the nature of the end user. For example, mobile medical apps (MMAs) can be designed for sale directly to consumers for health and wellness purposes or they can be directed at provider customers as a means of helping providers improve the quality of patient care or of the care experience. The data being collected in each instance and the privacy and security needs associated may be different and impact the potential risks to privacy and security identified during a risk assessment. In terms of documentation, FDA's quality systems regulation, including good manufacturing practices (GMP), also have implications for device security. Those requirements include design validation, including procedures appropriate to the intended use and to the user and patient. The FDA requirements also include validating and documenting the software used and a documented system of correction and preventions for any quality problems, which would include security inadequacies.

2. **Regularly review and update privacy and security protocols.** The privacy and security of health information and other types of personal information is not limited to the design process, it continues throughout the lifecycle of the device or application. In addition to conducting an initial privacy and security review, make sure it is updated periodically to account for new potential risks as well as any changes made to the device or the manner in which it is marketed and used in the marketplace. Conduct testing to identify any lingering vulnerabilities, such as "backdoors" inadvertently left by developers. If you are using third-party code or modules, investigate and address potential third-party security vulnerabilities. For MMAs, FDA requires investigation into, and documentation of, the quality assurance systems of suppliers and consultants, but all medical device manufacturers and application developers should make sure to conduct due diligence on their privacy and security controls. Any potential vulnerabilities found or recommendations made during the review process should be evaluated and either implemented, or if they cannot be implemented for some reason, mitigating controls should be implemented to reduce potential privacy or security risks.

3. **Be aware of, and plan for, data collection.** Consistent with the idea that one size does not fit all, decide what data will be collected by the application or device, why it will be collected (i.e., what is the business need?), who will the information be disclosed to, and how the

information will be safeguarded. Depending upon the circumstances, the application or device could be subject to a range of privacy and data security laws and regulations. For example, where the device or application will be collecting patient protected health information or warehousing it, does your organization have a program in place to comply with the HIPAA privacy and security rules? Minimizing what data is collected and retained is a key means of minimizing potential risk. In fact, the FTC encourages data minimization as a means of mitigating threats particular to data. Those include a breach or compromise of stored data; correlation of data as a means of re-identifying patients; unauthorized secondary use of data; disclosure or identification; and unauthorized surveillance or monitoring. Collecting only the minimum amount of information necessary also is consistent with the HIPAA privacy rule's "minimum necessary" principles. Exposure also can be reduced by only retaining identifiable information as long as necessary to satisfy legal obligations or the reasons for which the information originally was collected.

4. **Stay informed about and current with best practices.** Stay abreast of industry privacy security resources and tools, from guidance from FDA, HHS, the FTC and other regulators to information concerning known vulnerabilities and threats, to standard-setting organizations and what are considered best practices. Encryption is an important potential means of safeguarding the privacy and security of health information, as well as a means of minimizing the potential for a data breach in the event that an unauthorized third party compromises your organization's systems. Techniques such as rate limiting to prevent brute force Internet attacks also should be considered as another example of best practice. Password protection by itself is rarely going to be enough. Especially for sensitive health data of the sort often collected by medical devices and applications, look at encrypting that information and the use of multi-factor authentication as opposed to a static password. Nor is one mode of security sufficient or simply addressing security vulnerabilities one time at the design phase. Good security is multi-level, and the prudent medical device manufacturer will evaluate security risks and make adjustments and updates as necessary on an ongoing basis.

   A special word is warranted about Internet connectivity. Protection against the use of remote Internet-based access to medical device controls is essential. The FTC has warned of the potential problems here, having reported specifically on risks associated with the Internet of Things. Those include threats to patient safety and using Internet-connected devices as a springboard to launch attacks on other systems. One need only consider examples like unauthorized remote access to an insulin pump or heart rate monitor to appreciate the seriousness and multiplicity of possible threats.

5. **Create a culture of privacy and security.** An understanding about, and emphasis on, data privacy and security should be woven into the entire fabric of the organization. Training on privacy and security and the importance of implementing internal controls — addressing the human factor and the possibility of human error or bad intention — remains critical. A successful training program will go a long way not only to prevent incidents, or at least minimize the chances of a security breach, but also help establish that your company's privacy and security procedures for the health information that your organization collects through its medical devices or applications are reasonable. Not to be forgotten are recent examples of data breaches arising from something as simple, and as harmful, as a lost or stolen laptop or other data-bearing device. If there is any regulatory audit or investigation, training will also help in establishing that the company implemented reasonable precautions.

   In one well-publicized case that resulted in a long-term and expensive set of requirements for mobile device manufacturer HTC America, the FTC charged the company with the failure to employ reasonable and appropriate security measures. Among the failings were lack of security training for the engineering staff, no review or testing of software for security vulnerabilities, failure to follow secure coding practices, and failure to implement a third-party reporting mechanism.

6. **Incorporate security responsibilities into your contracts.** Don't forget about your service providers and your customers. Especially for medical device manufacturers in the complex and multi-actor continuum of care, it is important to make sure that there is clear contractual allocation of responsibility for safeguarding personal information and also procedures for who handles privacy and security problems when they arise. This means looking at both your agreements with your vendors/service providers as well as your agreements with your direct

customers or end users. It includes notifications about data breaches. What do you tell someone or your customer when there is a breach? And you need to address security updates. What time limits are in place concerning when patches and updates need to be provided? It can be risky to leave that undetermined and open-ended. Finally, be sensitive to what representations you may be making, directly or indirectly, about the security of your products and their privacy protections.

Remember that privacy and security is an ongoing and evolving process, where regular maintenance and attention is the goal. This is hard work, but the attention is well-warranted.

Authors and Contributors

Kevin Coy
Partner, DC Office
202.677.4034
kevin.coy@agg.com

Andrew B. Flake
Partner, Atlanta Office
404.873.7026
andrew.flake@agg.com

not *if*, but *how*.®

About Arnall Golden Gregory LLP

Arnall Golden Gregory, a law firm with more than 150 attorneys in Atlanta and Washington, DC, employs a "business sensibility" approach, developing a deep understanding of each client's industry and situation in order to find a customized, cost-sensitive solution, and then continuing to help them stay one step ahead. Selected for The National Law Journal's prestigious 2013 Midsize Hot List, the firm offers corporate, litigation and regulatory services for numerous industries, including healthcare, life sciences, global logistics and transportation, real estate, food distribution, financial services, franchising, consumer products and services, information services, energy and manufacturing. AGG subscribes to the belief "not if, but how.®" Visit www.agg.com.

Atlanta Office
171 17th Street, NW
Suite 2100
Atlanta, GA 30363

Washington, DC Office
1775 Pennsylvania Avenue, NW
Suite 1000
Washington, DC 20006

To subscribe to future alerts, insights and newsletters: **http://www.agg.com/subscribe/**