Using Information Governance to Avoid Data Breaches and Provide Cybersecurity

By Gail Gottehrer, JD, and Ronald J. Hedges, JD

The seemingly daily announcements of cyberattacks and data breaches underscores the need for effective information governance (IG), particularly in the healthcare industry.

Consider a situation in which a healthcare provider learns that a wearable device approved by the Food and Drug Administration (FDA) that transmits patient data directly to the provider needs a software update. That device, which collects data through sensors worn on the patient's body, is used for treatment purposes. No other information is available from the manufacturer or the FDA. How the provider responds to the risks created by this situation is a valuable test of its IG program. Working through 10 key IG competencies can help the provider decide how to proceed. That process will also identify potential weaknesses in the IG program and areas for improvement.

IG Structure

An IG program could be expected to anticipate issues such as the above, as well as have procedures and policies in place to address it. The policy could be that a designated employee sets their computer to constantly search the internet, including blogs and social media sites, for references to the technologies used by the provider, and have the computer automatically alert the employee when it finds something of note. That way, the provider becomes aware of possible problems with the technology as early as possible and can respond quickly, rather than first hearing about the problem from the manufacturer or the FDA. The policy could further provide that when the employee is alerted to a possible problem with a technology, they inform a committee of senior-level stakeholders. That committee should be set up in advance, with members that meet on a regular basis to discuss how to handle these situations.

Strategic Alignment

A well-aligned IG program should be prepared for the situation described above because it would enable the use of technology and data for patient care, as that is the goal of many IG programs. If the IG program has not been designed to identify and respond to scenarios like this, it exposes the provider to potential liability and financial and reputational damage.

Privacy and Security

The provider's chief technology officer (CTO), chief information security officer (CISO), and chief privacy officer (CPO)—to the extent the provider has one or more of these C-suite positions—and their teams will play a critical role in ascertaining the scope of the risk and the questions that must be answered in order to recommend a course of action.

Those questions could include:

- Is the information being collected by the devices and transmitted to the provider accurate?
- Has the data been compromised or altered before or during the transmission process?
- Does the incoming data from the devices pose a threat to the provider's computer systems?
- Is the provider's computer network, and the data on it, infected with malware?
- Is information being shared improperly?
- Do medical experts need to be consulted to determine if there is an ongoing threat to patients and if the technology issue could be interfering with their treatment?
- Is there a chance that the problem that is causing the manufacturer to update its software could lead to a HIPAA violation, such that the legal department needs to be consulted?

Legal and Regulatory

Senior members of the provider's legal and compliance departments should be members of the committee set up as part of the IG program to address high-risk situations like this one. They will assess the provider's legal exposure, the legal and regulatory obligations it may have, and the available legal remedies. The questions they will focus on may include: Is there reason to believe that whatever led the manufacturer to need to update its software requires the provider to notify patients or regulators of a breach? Has something happened that requires, or makes it advisable for, the provider to discontinue its use of the technology? Do medical ethicists need to be consulted? Does the provider's insurance carrier need to be notified of the situation? Does the manufacturer have a contractual obligation to provide additional information to the provider? Is the manufacturer in breach of that contract? What causes of action might the provider have against the manufacturer, and what damages might the provider be able to recover? Are there any steps that need to be taken at this time to ensure the viability of claims the provider may have against the manufacturer and to preserve electronically stored information (ESI) and other data sources that may be relevant to future litigation associated with this situation?

Data Governance

The team members responsible for data governance (which could be the CTO, CISO, CPO or members of their staffs), will be in the best position to know where the data transmitted by this technology is stored by the provider, how it is used, and who has access to it. The IG program should define their role. This could include identifying everywhere the data resides, which may be on the provider's computer network and in the cloud or other offsite storage. Data governance team members would also determine whether the data has been shared with other entities, and if it has, who it has been shared with in case those entities need to be notified. Additionally, this professional would know which medical personnel have accessed and used the data, as well as know which patients are being treated using this data.

IT Governance

A central feature of a medical provider's IG program is likely to be policies and procedures for selecting, evaluating, and using technology in an effort to reduce risk. As a result of these policies, the provider should have documentation detailing the reasons why the technology at issue was selected; what potential risks were identified during the vetting process; whether a problem like this one was considered and if so, if a backup plan was created; and whether there are other vendors who manufacture similar technology and could be alternative providers in the event the provider decides to stop using the technology and switch manufacturers.

Analytics Tools

As part of the IG program, analytics tools can be used to identify trends and anomalies in the data from technologies like the one at issue here. Through analytics, the provider can look at the data from this technology over a period of time and see if there have been problems in the past, if there are reasons to believe the data generated by the technology may not be reliable, and whether any patterns emerge. This can provide additional information to help the provider assess the level of risk posed by the technology and the manufacturer's software update.

Enterprise Information Management

By putting procedures in place to track information as it travels across the healthcare ecosystem, the provider's IG program will enable it to determine which doctors, nurses, pharmacists, lab technicians, members of the health information management department, and other personnel use this technology, or rely on the data generated by it, and may need to be made aware of the potential problem. It may reveal whether there have been complaints about the technology or the integrity of the data received from the devices, or if the data generated by the technology has been shared with other entities, used for research purposes, or used in publications.

IG Performance

The performance and impact of the provider's IG program will be revealed as the provider works its way through the process of evaluating how to respond to the news of the manufacturer's planned software update. If the IG program is effective, the provider should be able to access the information it needs to weigh its risks and options in a timely manner. If the process turns out to be slow and complicated, with employees being uncertain about their responsibilities and unable to locate the necessary information, that will indicate that the IG program is not performing as intended and needs to be overhauled.

Awareness and Adherence

The process of reviewing internal data to respond to this potential threat will also allow the provider to evaluate whether, and to what extent, employees are aware of its IG policies and procedures, and whether they are following them. This exercise will show whether IG policies were known to employees; whether they were followed; whether additional training is required on certain policies for certain employees; whether the data from the technology at issue was used appropriately; whether it was shared only as specified in the IG policies; whether the appropriate access restrictions were in place; whether data security and privacy were maintained; and whether the data was disposed of in accordance with the provider's records retention schedule.

Healthcare providers must expect to be confronted with—and integrate—new technologies for the care and treatment of patients on a regular and accelerating basis. As this article demonstrates, an information governance framework provides a method to address new technologies and cybersecurity risks that these technologies may present.

Gail Gottehrer (ggottehrer@outlook.com) is the founder of the Law Office of Gail Gottehrer LLC. Ron Hedges (r_hedges@live.com) is a former US Magistrate Judge in the District of New Jersey and is a writer, lecturer, and consultant on topics related to electronic information. He is a senior counsel with Dentons US LLP.

Article citation:
Gotteher, Gail and Ron Hedges. "Using Information Governance to Avoid Data Breaches and Provide Cybersecurity." Journal of AHIMA 90, vol. 4 (April 2019): 30-31.