IT Systems Put Security into Health Care Cybersecurity

As Health Care Organizations Increasingly Depend upon Connected Devices, Security Must Be Front and Center

William A. Tanenbaum

Strong cybersecurity is no longer an option for health care institutions. A medical chart is identity theft on a platter. Criminals pay more for personal health information than for credit card numbers. Unauthorized access to electronic health records surpassed hacking as the chief cybersecurity risk in 2016. Third-party information technology (IT) systems used by heath care providers and other institutions (referred to for convenience as "hospitals" in this article) are a key avenue of unauthorized access and pose a significant risk as hospitals upgrade IT systems either alone or as part of a merger into larger health care systems. This article address how health care IT puts the security in health care cybersecurity.

William A. Tanenbaum is the leader of the Health Care IT practice at Arent Fox LLC and co-head of the firm's Technology Transactions Group. In 2016, he was named as one of the Top 5 IT lawyers in the United States by Who's Who Legal, and he was previously named as the Lawyer of the Year in IT in New York by US News & World Report/Best Lawyers.

Seven Critical Cybersecurity Roles Played by IT

Once a hospital establishes rules for the access and use of health care information based on regulatory rules (such as the Health Insurance Portability and Accountability Act (HIPAA)) and institutional data protection requirements, they are implemented through IT systems. IT systems determine whether or not an individual or company working with a hospital is authorized to access, use, and transmit electronic health records. This is especially important in health care because different professionals use different personal health information for different purposes. This makes privacy contextual, and data protection for information stored in hospital IT and database systems must be tailored to the context for both regulatory and data security reasons.

The flipside of controlling access by hospital professionals is controlling access by external parties. External parties can be outsourcing vendors and other IT vendors and others with permission whose access must be controlled, and third parties with no permission — such as hackers and criminals — whose access must be prevented.

The above illustrates the critical cybersecurity functions enabled through IT. These are:

1. risk and compliance with management, including with regulatory compliance;
2. identity authorization and access management;
3. identifying and remediating security violation occurrence;
4. intrusion detection (detecting unauthorized access, especially by external parties, to hospital systems) and using technology to protect against intrusions;
5. data encryption, both when the data is being transmitted and when the data is "at rest" in the storage media;
6. protecting the security of the hospital IT system through the use of antivirus and antimalware technology; and
7. data integrity and protecting data against unauthorized changes.

Third-Party IT Provides a Pathway for Cyber Attacks

Hospitals generally use three methods of acquiring an IT system, and often use a combination of them. The first is to purchase hardware and license software from hardware and software vendors. These vendors may in turn be integrators of hardware and software systems acquired from other providers. The second is to use one of the various forms of outsourcing. Here, the outsource vendor owns, runs, upgrades, and takes responsibility for operating hardware and software systems in place of the hospital doing so itself. The third method is the use of cloud-based systems, which is at least in part a form of outsourcing. Cloud computing is not just a storage system; it is also a platform to host the hospital's data and software systems. Of course, cloud vendors often provide services and deliver "output" to hospitals.

The risk is that outsourcing and third-party vendor IT systems provide an avenue for cyber attacks. Many well-known breaches of retail business were achieved through successful attacks on third-party vendor systems. In one case, by finding a hole in those systems, the criminals were able to exploit that hole to access data stored on the business core databases. In another notable case, the IT outsourcing vendor left a temporary "back door" into the system for its convenience in preparing the system for "go live" use. When the vendor neglected to close the access after go live, criminals used the access to steal credit card numbers.

Hospitals updating their IT systems and using third-party vendors, outsourcing, or cloud service vendors to do so need to guard against their third-party vendors providing the on-ramp for data theft. This is where the difference between best practices and best of breed practices becomes important. A hospital that is measuring the cybersecurity strength of its IT systems against other hospital IT systems may be seen to follow best industry practices even though it may be following a practice with known weaknesses.

A better course is to follow "best of breed" practices regardless of the industry that developed those practices. For example, financial institutions have had long experience developing IT systems to protect personal information in a regulated environment. Accordingly, hospitals do not need to reinvent the IT wheel on all aspects of IT data security. Instead, hospitals can adopt practices from the financial services industry that are sophisticated and provide well-developed protection against unauthorized third-party access. For example, the customer, here the hospital, will enter into IT agreements with strong security audit rights to verify the integrity of the third-party systems. The audit rights include testing the system for security holes and requiring the vendor to show ongoing and current compliance with security certifications.

Connected Devices Should be the "Security of Things" Not Just the "Internet of Things"

From an IT perspective, hospitals are premier users of the "Internet of Things,"

and patient care and hospital administration will increasingly depend upon "connected devices." Wearable medical devices, implanted medical devices such as pacemaker and other devices used to provide patient care are connected over a network. Hospitals also use network connected devices that are not used as part of direct medical care. However, without protection, devices that are connected over a network can be hacked through the network. Thus, the hospital "Internet of Things" should be the "Security of Things."

To accomplish this, hospitals should be aware that many vendors of connected medical devices do not bake security features into the devices. This is a risk that should be identified during the Request for Proposal (RFP) process. For this reason, vendors who are focused on new healthcare IT devices, and not adopting preexisting technology to the hospital setting, may have better cybersecurity protocols from day one. Even if the individual devices themselves are secure, data being transmitted between devices may be hacked while in transit. In addition, where the connected devices cannot be upgraded by a centralized IT system, they may need to be upgraded manually one at a time. The logistics of this are daunting and introduce a security vulnerability. In selecting a vendor, the hospital needs to know how the vendor will upgrade the systems (centrally or manually) and at what cost and at what speed. This is especially important when an adverse line of attack is developed by hackers and the hospital needs to update security quickly to meet a new risk.

Because connected devices create special cybersecurity problems, special IT measures should be taken. IT infrastructure and network design can minimize the risks of connected devices. For example, connected medical devices should be isolated on the network from other devices. Because hacking a medical device can do harm to a patient, segmenting medical devices from other devices on the network reduces avenues of cyberattack to the medical devices. This segmentation may well conflict with another IT goal of interoperability of all elements of the IT system. Medical devices differ from other connected devices in that they directly affect health, and hospital network design needs to take into account health care-specific balancing of risks and benefits.

IT Cybersecurity Starts at the RFP Stage

Using IT systems to provide cybersecurity protection starts at the RFP stage. The first step in acquiring IT for the hospital (often in combination with consulting and law firm advisors) is to issue an RFP.

The RFP is where cybersecurity protection begins. To accomplish this, in preparing the RFP, the hospital should, with assistances of advisors if necessary, prepare a list of security requirements and require the potential vendors to indicate in their RFP responses how the security requirements will be met. In fact, the technology and subcontractors identified in the RFP response will often provide the hospital with good insight into the strength of cybersecurity protection it will obtain from a vendor. A good, practical practice is to provide the vendors with the opportunity to ask questions to get additional information about the requirements and structure their responses to target the hospital needs. Cybersecurity should be part of this phase.

RFP responses are evaluated using a score card to measure and compare vendor responses on various criteria. In creating the score card, hospitals should guard against valuing price over cybersecurity. This is to protect against the RFP process inadvertently penalizing a vendor which proposed robust cybersecurity technology and practices. Strong cybersecurity requires ongoing investments by IT vendors (including cloud vendors). These investments will be part of a vendor's price proposal, and fairly speaking, they should be. Physical and "logical" security

requirements should be part of the RPF. Physical security is securing the locations where computer systems are placed against access by unauthorized personnel, including both hospital and vendor staff who lack a "need to know" reason for access. Physical security also includes protection against loss and unauthorized use of laptops with sensitive data. Consultants still lose laptops or have them stolen from cars. "Logical" security is essentially electronic security and other automated security features embodied in the IT and computer systems. It also includes the proper use of the proper encryption.

Another factor in using RFPs for selecting a vendor with strong cybersecurity is involving relevant hospital professional staff, and at the right stages in the RFP process. For example, in addition to the CIO, the Chief Information Security Officer and the Chief Data Officer should be part of the process. They should be involved in determining the criterial cybersecurity and data integrity, and in scoring vendor responses against these responses. Involving these professionals only after the finalist vendors have been selected may result in selecting a final vendor from a pool of finalists which did not offer the strongest security offerings. This in effect prejudices the outcome of the vendor selection process.

The desired outcome of the RPF process is to select the right vendors and enter into contracts that provide the right incentives to the vendor and the right protections and remedies for the hospital. A time- and cost-effective means of achieving this is in the legal realm. Lawyers should ensure that RFPs are designed so that the vendor responses can be easily converted into the right part of the contractual documentation. It is also beneficial to have the RFP and the contract written so that specific subject matter appears in one place and is not spread throughout the documentation. For example, all cybersecurity should appear in a single section or document in both the RFP and in the final agreement. This makes it easier for the hospital cybersecurity team to evaluate vendors on the cybersecurity criteria. At the contract stage, it makes it easier for the hospital cybersecurity team to administer the contract and measure vendor data protection performance. Having the RFP map to the contract avoids renegotiation with vendors at the contract stage. The hospital will have had greater leverage at the RFP stage; therefore, that is the best point at which to have vendors lock in to meaningful cybersecurity practices.

Having a vendor voluntarily withdraw early in the RFP process because it has concluded that it will not be able to meet the contractual levels of cybersecurity benefits the hospital in two ways. Unqualified vendors disqualify themselves, and this in turn allows the hospital to focus its limited time and budget on qualified vendors. This is both a consequence of and a reason to have detailed rather than high-level data security requirements in the RFP.

Most vendor agreements consist of a Master Services Agreement (MSA) and individual Statements of Work (SOWs) that apply to specific projects conducted under the framework established by the MSA. Most disputes arise under an SOW and not the MSA. Since the SOWs are contractual as well as technical documents, SOWs should be reviewed and modified as necessary by lawyers to protect the hospital in the event of a dispute. A successful SOW gives rise to a "silent win." That is, in the event of a dispute over whether the vendor has performed in accordance with requirements, the vendor's accountant manager or lawyer will read the SOW and decide the vendor will not prevail in dispute. In that case, the SOW resolves the dispute in the hospital's favor at the very beginning of the disagreement.

Good IT Contracts Lead to Strong IT Systems

Contracts play a role in IT security in designing IT systems to implement security

requirements. IT contracts should require connected device vendors to routinely identify security vulnerabilities. This can go as far as requiring "white hat" hacking to discover the weakness before "black hat" malevolent hackers discover them. The vendor itself can conduct white hat hacking, or special forensic companies can conduct the security verification. From the hospital perspective, discovering vulnerabilities before criminals do is the best step to cybersecurity. Therefore, the hospital should not penalize vendors for uncovering vulnerabilities — especially to newly created threats — and should use the contract provided requirements and incentives to do so and not penalize vendors for upgrading the system. From a patient safety and operational point of view, this is better than having a vendor hide the weakness and hoping it is not found to be in breach of the contract. Here is where the contract should be an early warning system to identify and remediate problems quickly, but it must be written with special provisions in order to accomplish that.

The summary of steps hospitals can take to use IT to provide cybersecurity and prevent unauthorized use of medical information is as follows:

Critical Cybersecurity Roles of Health Care IT

- Use robust IT systems to prevent unauthorized access, use, and transmission of health care data.
- Privacy and authorized use depends on the context.
- Use IT to enforce different authorization rules based on the context of who needs what information for what purpose.
- Use IT to detect and prevent intrusions.

Third-Party IT Provides a Pathway for Cyber Attacks

- Recognize the risk of third-party IT systems providing an unintended pathway to hospital patient health information.
- Use robust contracts and verified IT systems to protect against the risk.
- Audit network operations.

IT Cybersecurity Starts at the RFP Stage

- Include specific cybersecurity requirements to generate meaningful vendor responses.
- Do not overvalue price at the expense of strong cybersecurity in the RFP scoring process and vendor selection.
- Involve the right hospital professional staff at the right points in the process.

Connected Devices Should be the "Security of Things," Not Just the "Internet of Things"

- Be wary of connected devices which do not have security baked in.
- Take advantage of new IT vendors if they have stronger security.
- Determine how connected devices will be upgraded to keep current with security threats.
- Isolate medical devices on the network to prevent authorized access to the network from gaining access to medical devices where patient health can be affected.
- Identify trade-offs required between interoperability and segmentation of medical device connected networks.

Good IT Contracts Lead to Strong IT Systems

Use contracts as early warning systems to uncover and remedy IT cybersecurity risks at an early stage.

- Favor early identification of cyber risks over contractual disputes.
- "Legalize" SOWs so they provide the rights and remedies found in a contract and thus provide protection to a hospital that a purely technical project plan will not.

Conclusion

Regulatory compliance and adherence to hospital data protection rules become effective when they are embodied in good IT

systems. Internal IT systems in combination with systems provided by third-party IT vendors implement the key requirements of providing authorized, and prohibiting unauthorized, access to, and use and transmission of health care information. Privacy is contextual, and using technology that allows different hospital professionals to have different access to different data for different purposes to satisfy regulatory requirements, hospital policies, and protection against internal and external cybersecurity threats is the mark of a well-considered information technology cybersecurity plan. Using RFPs strategically will identify vendors who provide strong cybersecurity tailored to the hospital's specific requirements.

Reprinted from Journal of Health Care Compliance, Volume 18, Number 4, July–August 2016,
pages 21–26, with permission from CCH and Wolters Kluwer.
For permission to reprint, e-mail permissions@cch.com.