Hospital Hijacked – Lessons from Hollywood Presbyterian

Hospital administrators have hoped for years that a massive cyber attack/data breach nightmare was just that, a dream. Everyone hoped that this was a "could not happen to us" scenario; with the worst-case nightmares combining a *Die Hard*-style invasion and exclusion by outsiders with the modern hacking technology of today's cyber attackers, such as was leveled at Sony Pictures as revenge for its release of *The Interview* in late 2014. Alas, this cyber invasion nightmare is not fiction; it is exactly what happened to Hollywood Presbyterian.

Last week Hollywood Presbyterian Medical Center had its IT systems literally taken hostage by hackers. The hackers pierced security systems, took control of the system, excluding regular users entirely, and demanded that the hospital pay $3.6 million to regain control over its IT systems. This attack reportedly impacted healthcare as medical records, email, and other internal communications and record retrieval systems were rendered inoperable. The hospital cooperated with local and federal authorities as they worked through the fallout of the attack to provide quality medical care to patients. A small ransom was ultimately paid and the IT was restored, but the real life event is enormously disturbing.

Why Hollywood Presbyterian? Why a hospital at all? While some have speculated that its ownership by South Korean interests is as far as you need look to the answer, there are no facts, and no apparent motivations beyond the ransom demand. Accordingly, as best anyone can tell it is a nightmare that can happen to any hospital or large health facility of any kind.

While most Hospitals and major healthcare facilities have carefully implemented their IT security and security breach response plans, it is a propitious time to reassess both. Despite the advances in computer security, it is apparent that the current defensive measures available to well-meaning organizations are no match for cyber terrorists and ransom seekers. Accordingly, the response plan is an enormously important organizational survival tool, and needs careful thought and review.

The response plan has three defined sub-parts:

1. Recognition, identification, and remediation of the IT issues;

1. Appropriate notification to authorities, and

1. When required, notification to patients.

In implementing a response plan, diverse resources are brought to bear: forensic IT specialists, insurance specialists, legal compliance specialists, patient care leadership, and public communications specialists to name a few.

In focusing on the legal compliance aspects, the following issues rise to the top of the list:

1. Determine Whether a Breach Has Occurred

A "breach" is the acquisition, access, use or disclosure of protected health information (PHI) that is not permitted by HIPAA and that compromises the security or privacy of the PHI. An impermissible acquisition, access, use or disclosure of PHI is presumed to be a breach unless the covered entity or business associate demonstrates that there is a low probably that the PHI has been compromised.

2. Conduct a Risk Assessment

Upon discovery that a breach occurred, the covered entity or business associate must conduct a risk assessment to prove whether there is a low probability that PHI has been compromised. The risk assessment must assess the following factors:

- The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification?
- The unauthorized person who used the PHI or to whom the disclosure was made?
- Whether the PHI was actually acquired or viewed? and
- The extent to which the risk to the PHI has been mitigated.

The covered entity or business associate must maintain documentation of the risk assessment.

3. Comply with Federal and State Breach Notification Requirements

Following a breach of unsecured PHI, the organization must provide notification of the breach to affected individuals, the Secretary of Health and Human Services (Secretary), and in certain circumstances state agencies and the media.

Individual Notice

Covered entities must notify affected individuals following of a breach of unsecured PHI. Notification must be in written form by first-class mail, or alternatively, by email if the affected individual has agreed to receive such notices electronically. In certain circumstances, the covered entity must provide substitute individual notice by either posting the notice on its website or by providing the notice in the media where the affected individuals likely reside.

Individual notifications must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach. Individual notifications must include a description of the breach, the types of information involved, the steps individuals should take to protect themselves from potential harm, a description of what the organization is doing to investigate the breach, mitigate the harm, and prevent further breaches, and contact information of the organization.

A covered entity may delegate the responsibility of providing individual notices to a business associate where the breach occurred at or by a business associate.

Media Notice

If a breach affects more than 500 residents of a State or jurisdiction, the covered entity or business associate is required to provide notice in a prominent media outlet serving that State or jurisdiction. This notification must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include the same information required for individual notice.

Notice to the Secretary

Covered entities must also notify the Secretary of breaches of unsecured PHI through the HHS website. If a breach affects 500 or more individuals, notification must be provided without unreasonable delay and in no case later than 60 days following a breach. If a breach affects fewer than 500 individuals, notification may be provided on an annual basis, no later than 60 days after the end of the calendar year in which the breach is discovered.

California Breach Notification Requirements

In California, a business must notify any California resident whose unencrypted PHI was acquired, or reasonably believed to have been acquired, by an unauthorized person. Notification must be made in the most expedient time possible and without unreasonable delay. The breach notification must be written in plain language, include the title "Notice of Data Breach," and present information under the following headings: (1) What Happened; (2) What Information Was Involved; (3) What We Are Doing; (4) What You Can Do; and (5) For More Information. If the breach involves more than 500 California residents, the business must electronically submit a single sample copy of the security breach notification, excluding any personally identifiable information, to the California Attorney General. Additionally, a clinic, health facility, home health agency, or hospice must report any unlawful or unauthorized access to, or use or disclosure of, a patient's medical information to the California Department of Public Health no later than 15 business days after the unlawful or unauthorized access, use, or disclosure has been detected by the clinic, health facility, home health agency, or hospice.

Healthcare facilities of all types should review how they would be able to respond to the threat that materialized with Hollywood Presbyterian.

For more information/questions regarding any legal matters, please email info@nelsonhardiman.com or call 310.203.2800.

Article co-authored by Rob Fuller and Kathryn Russo.