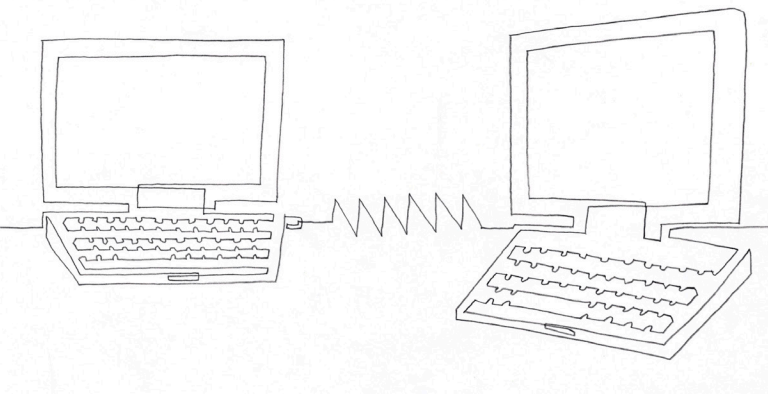
Beazley Insight
The Case of the $1.7 Million Laptop

by Sue Yi



The Case of the $1.7 Million Laptop

by Sue Yi

Federal regulators are serious about data privacy. Two recent announcements from the Department of Health and Human Services signal a new tough stance on guarding patient information and, in particular, on encrypting portable electronic devices.

The announcements settled cases against Concentra Health and QCA Health Plans and called for substantial payments — $1.7 million for Concentra and $250,000 for QCA — as well as extensive correction programs. They stemmed from the loss of just two unencrypted laptops.

What exactly is encryption? What are the rules? What do these two cases tell us? And how should health care providers respond?

Encryption is the process of encoding or "scrambling" a message in such a way that the information becomes indecipherable to an unauthorized recipient. The message or information is encrypted using an algorithm that renders it unreadable. Only an authorized recipient, using a key, can convert it back into usable text.

HIPAA's Security Rule is clear: Any electronically stored patient information must be safeguarded by encryption or an alternative reasonable means. If an organization does not encrypt, it must document its decision and the reasons it was deemed not reasonable and appropriate.

In Concentra's case, the settlement showed that Concentra Health knew that 163 of its 597 laptops were unencrypted. As luck would have it, the laptop stolen from Concentra ended up being one of the unencrypted devices. The investigation, by HHS's Office for Civil Rights, revealed that Concentra did not take steps to encrypt this known inventory of unencrypted laptops. On top of that, Concentra did not document its reasons for failing to encrypt, nor did it adopt a reasonable alternative safeguard.

OCR did not look kindly on this. Ultimately, as a result of the investigation, Concentra agreed to a $1.7 million settlement payment as well as a burdensome and lengthy corrective action plan that can expose Concentra to additional penalties.

QCA Health Plans reported the theft of an unencrypted laptop from an employee's car; an incident that affected only 148 individuals. Despite the low number of individuals affected, QCA paid $250,000 to settle potential violations of the HIPAA Privacy and Security Rules.

The Office of Civil Rights found that QCA had failed on a number of other fronts. They were systematically non-compliant. QCA didn't establish a security program; they didn't properly assess the risks of using Electronic Patient Health Information (ePHI) and they didn't physically guard their equipment.

Doing the math, QCA settled for about $1,690 for each lost record—a hefty sum per person affected, and a cost that would have easily been avoided had the laptop been encrypted or proper security procedures put in place.

Looking at the bigger picture, the cost of encrypting a single laptop can be as low as $100. And larger institutions can obtain volume discounts, which can, at times, drive down costs to as low as $50 to $80 per device.

The message is clear. It makes sense to make sure every single device – without any exceptions – is encrypted. Or, as an alternative, to document the reasons for a different approach. And as the OCR explained in the QCA Health Plans case, a company has to have an established safety program.

Looking at Concentra Health, it's worth noting that they had already invested in encryption for nearly three quarters of their portable devices. They could have brought the rest into compliance for a fraction of the ultimate cost. Instead a single stolen laptop cost the company $1.7 million.

Sue Yi is a Privacy Breach Response Services Manager in the Specialty Lines division of Beazley Group. This article was first published in the Risk Management Monitor.

Sue Yi
Privacy Breach Response Services Manager
Philadelphia, PA
sue.yi@beazley.com

CBSL359_US_12/14

beazley