Privacy in Health Care

The world of health care moves fast. Hospitals, physicians and other providers must protect the confidentiality of health information in a highly regulated environment with constantly evolving technology. How can you address privacy breaches and be ready for HIPAA audits? Ice Miller can help.

300+ lawyers in Illinois, Indiana, Ohio and Washington, D.C.
100+ lawyers from Ice Miller recognized by Best Lawyers in America®

protect confidentiality

A Breach, or Not a Breach?
If That Is the Question, Encryption May Be the Answer

How the definition of a data breach can cause regulatory trouble and cost money
Since the passage of the HITECH (Health Information Technology for Economic and Clinical Health) Act in 2009, the unauthorized disclosure of protected health information (PHI) continues to be a significant risk for health care providers and patients. Statistics maintained by the Department of Health and Human Services (HHS) for large data breaches (those affecting more than 500 people), and analyzed in a report by the health care information security company Redspin, indicate that in 2013 alone there were 199 breaches affecting over seven million patient records.

A look at the breach statistics reveals several patterns, but one is especially glaring: the largest single source of PHI breach is the theft or loss of portable (or moveable) devices – desktop computers, laptops, portable drives. In 2013, there were 100+ such incidents that accounted for over 85% of the total patient records affected, or more than six million records.
One precaution can determine if a “breach” occurred

It may surprise you to read that none of these incidents would even have been considered a “breach” under the modifications of the HIPAA breach notification rule that went into effect in January 2013 if the covered entities or business associates possessing the information had taken one precaution. They would not have had to be reported to HHS, nor would the rule’s notification requirements have applied. What was the one thing the providers could have done to make their breach problems go away? They could have encrypted the data.

Applying the breach notification rule

To understand this notion, let’s back up a couple of steps. The breach notification rule states that the reporting and notification requirements only apply if the PHI was “unsecured.” PHI is unsecured if it has not been rendered “unusable, unreadable, or indecipherable to unauthorized individuals” by either encrypting or destroying it through the use of technology approved by the HHS Secretary. Thus, if the information that was subject to unauthorized disclosure had been encrypted, it would not be “unsecured” under the rule, and the unauthorized disclosure would not be considered a breach. (Note that most states with data breach statutes have a similar exception for data protected by encryption and other technical controls, but some do not.)
**Encryption is not password protection**

As you may already know, encryption is not the same as password protection. It’s a good idea to use a password to protect any device that contains PHI, but that is not sufficient to protect the PHI from unauthorized access. Passwords are relatively easy to defeat, and if they are defeated, the device’s data are wide open unless the data themselves have been encrypted using “an algorithmic process in which there is a low probability of assigning meaning without use of a confidential process or key,” and the key itself has not been breached.

**Encryption is not mandatory, but it is encouraged**

Encryption is not mandatory under the HIPAA Security Rule – it is an “addressable” element, meaning that a covered entity should consider doing it. But it’s a fair reading of the rule that if a covered entity “addresses” the issue of encryption and decides not to do it, the entity has to provide other compensating security measures that adequately protect its data. And if the entity’s compensating security measures prove ineffective – if, for example, a computer containing unencrypted PHI is lost or stolen – then the covered entity has a breach on its hands.
The burden of encryption or the burden of a breach?

The single largest PHI breach in 2013 involved the theft of four desktop computers from an office; the computers contained more than four million patient records. The additional burden of encrypting that data almost certainly pales in comparison to the burden of notifying millions of patients, going through the investigation and monetary penalties that will probably result, and defending the class action lawsuit that has already been filed.

Another example: in late April 2014, HHS announced that it had settled a breach enforcement action involving one stolen laptop and over 850 patient records. HHS’s investigation included the finding that the health care provider had previously recognized that the information on its computers and other devices needed to be encrypted, and it had started to do that, but its efforts were “incomplete and inconsistent over time, leaving PHI vulnerable throughout the organization.” And obviously, the laptop that was stolen had not yet been encrypted. The amount of the settlement is eye-catching: $1.7 million. Other reports about this large settlement have surmised that its size may have been related to the fact that this laptop loss was not the health care provider’s first; another laptop had been stolen about two years earlier. Whatever the reason for the high settlement figure, it graphically illustrates the risk.
Guidelines to assess if a breach has occurred

Nevertheless, if you are a covered entity that chooses not to encrypt its PHI, here are some guidelines under the breach notification rule to help you assess whether a breach has occurred, and therefore whether the notification requirements apply.

A breach is defined in the rule as an impermissible use or disclosure of PHI that “compromises the security or privacy of the protected health information.” A previous version of the rule stated that “compromising security or privacy” meant that there was a significant risk of harm to the patient – whether financial or reputational. This harm standard has now been discarded in the current version of the rule.

Four factors of risk assessment

The current version of the rule presumes that the impermissible use or disclosure is a breach unless the covered entity demonstrates, by doing a risk assessment, that “there is a low probability that the protected health information has been compromised.”

The risk assessment must consider at least four factors:

1. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification.

2. The unauthorized person who used the protected health information or to whom the disclosure was made.

3. Whether the protected health information was actually acquired or viewed.

4. The extent to which the risk to the protected health information has been mitigated.

For example, if a hospital’s medical records department faxes a medical record to the wrong physician, but the physician calls the hospital promptly to say she has recognized the error and immediately destroyed the misdirected record, the hospital will probably be able to demonstrate, through its risk assessment, that there is a low probability that the PHI has been compromised. In this example, the receiving physician’s prompt destruction of the misdirected record is good evidence that it was not viewed completely and that the risk to the PHI was mitigated (factors 3 and 4 of the assessment).
Three exceptions to the definition of “breach”

After the risk assessment establishes the facts related to the impermissible disclosure, the covered entity may find that one of three statutory exceptions to the definition of “breach” applies:

1. The unintended access or use of the PHI by an employee of the covered entity, acting in good faith within the scope of her authority.

2. The inadvertent disclosure of PHI by a person who is authorized to use PHI to another authorized person (this exception probably encompasses situations where the second authorized person did not actually “need to know” the particular PHI).

3. The disclosure to a person that the covered entity believes in good faith was unlikely to retain the information (example: a nurse in a physician’s office accidentally gives a medical summary to the wrong patient, who immediately sees that it is not hers and gives it back to the nurse).

If the covered entity’s risk assessment leads to the conclusion that an exception does not apply, and that it will not be able to demonstrate that there is a low probability that the PHI has been compromised – then the definition of “breach” has been met, the notification requirements kick in, an investigation will ensue . . . and the covered entity will probably start thinking wistfully about the virtues of encryption.
Resources

1. See http://www.redspin.com/whitepapers-datasheets

2. Information about which technology is so approved is provided in the document “Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals,” available at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html.

3. See 45 C.F.R. 164.304, available at http://www.ecfr.gov/cgi-bin/text-idx?SID=0dd6d19ecbab8288e94febb6898fa7c1&node=45:1.0.1.3.79.3.27.2&rgn=dv0.

Contact

Alan “Skip” Whaley
Partner
317-236-2362
Whaley@icemiller.com

Sherry Fabina-Abney
Partner
317-236-2446
Sherry.Fabina-Abney@icemiller.com

Robert Cochran
Of Counsel
614-462-2248
Robert.Cochran@icemiller.com

Stephen Reynolds
Partner
317-236-2391
Stephen.Reynolds@icemiller.com

Margaret Emmert
Of Counsel
317-236-2169
Margaret.Emmert@icemiller.com

Nicholas Merker
Partner
312-726-2504
Nicholas.Merker@icemiller.com

Christopher Sears
Partner
317-236-5891
Christopher.Sears@icemiller.com

© 2017 Ice Miller LLP