NEW DATA BREACH RULES HAVE BIG IMPACT

Small Changes – Big Impact

On January 25, 2013, the United States Department of Health and Human Services' Office of Civil Rights (HHS OCR) published the *Omnibus Rule* on HIPAA and HITECH amendments. While the proposed rule has been the subject to much debate, the final rule makes some changes which, while they appear to be minor, may have a major impact not only on HIPAA "covered entities", but also on business associates and their subcontractors who may have access to, or a need to use Personal Health Information (PHI.) The final rule and comments are more than 500 pages long, with sweeping commentary, and includes provisions making business associates and their subcontractors liable for compliance with HIPAA directly, new rules on healthcare marketing and fundraising, implementation of restrictions on the use of genetic information, new restrictions on the sale of PHI, and changes to the research exception and what entities with PHI have to do with respect to providing notice of privacy practices. The Omnibus Final Rule became effective on March 26, 2013, but covered entities and business associates have until September 23, 2013 to comply with certain provisions relating to business associate agreements that were in effect prior to January 25, 2013.

This white paper will seek to address only one primary change – how does the new rule impact information security incident response and data breach notification?

Scope of the Problem

HIPAA and HITECH have long required both covered entities and their business associates to provide notice when a data breach involving PHI was discovered, and provided a mechanism for such notification depending upon the number and character of the records breached. In general, covered entities were responsible to the data subjects (patients) for notification, and business associates were responsible to notify the covered entity that shared the PHI with them if the business associated discovered a breach. HHS has estimated that there will be 19,000 breach notifications just from covered entities annually (1,583 a month) affecting 6.71 million individuals.

The new rule subtlety but substantially changes the data breach regime in ways that could lead to substantial civil and criminal liability to covered entities, their associates and subcontractors. In particular, the new rule fundamentally alters the definitions of medical data "breaches" and the responsibility for investigating and reporting them. As such, it increases the need for both covered entities and their business associates to have a robust, comprehensive and documented security incident response, forensics and investigation capability.

New Definition of "Breach"

Prior to the amendments, HHS OCR defined a "breach" of PHI which would trigger a legal obligation to make a notification (either to the data subject, the public or HHS) to mean generally the acquisition, access, use or disclosure of PHI in a manner not permitted by the Privacy Rule which "compromises the security or privacy" of the PHI. But, under the old rule, not all violations of the Privacy Rule constituted a reportable "breach." An entity suffering a breach did not have to report it under what OCR called the "harm standard." If the unauthorized or improper access or use of the PHI did not pose a significant risk of financial, reputational or other harm to an individual, then notification was not required. In essence, "no harm no foul." The problem was different entities were taking vastly different approaches to what constituted a "significant risk of harm," leading many to not report breaches which should fairly have been reported. OCR responded by eliminating the "harm threshold" provision.

HHS now calls for covered entities and their business associates to assess the "probability that the PHI has been compromised" instead of assessing the risk of harm to the individual. The final rule notes:

> … an impermissible use or disclosure of PHI is "presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a **low probability that the protected health information has been compromised.**"

Under the prior rule, if there was a HIPAA violation which potentially exposed or misused PHI, but this violation resulted in no real harm to a patient or data subject, there was no need to report it. Under the new rule, there is a presumption that every HIPAA violation involving PHI (either use or disclosure) by either a covered entity or a business associate (or their subcontractors) is reportable. Moreover, under the new rule the entity must conduct and document an investigation in which it has the burden of proving that no PHI was compromised - a fairly high standard.

Impermissible USE or Disclosure

The new rule presumes that any impermissible use or disclosure of PHI is a breach. This is significant because it essentially presumes that any violation of any of the provisions of the Privacy or Security rules which then constitute an "impermissible use" of the PHI (a use in violation of the rule) constitutes a "breach" irrespective of whether or not the impermissible use caused or was even likely to have caused harm or damage to anyone.

An example illustrates why this is a substantial expansion of the rule. The HIPAA Privacy Rule requires both covered entities and their business associates to "make reasonable efforts to limit access to protected health information to those persons or classes of persons who need access to protected health information to carry out their duties and to disclose an amount of protected health information reasonably necessary to achieve the purpose of a disclosure." This seems reasonable in the abstract, but is frequently difficult to achieve in the real world. If a patient is admitted to a hospital for treatment, not only may doctors and nurses need to have access to their PHI for diagnosis and treatment, but nutritionists, cleaning crews, and even the HVAC technicians may need to have access to some PHI (if the patient is immuno-suppressed, air flow may go out but not in; if contagious, the other way around.) Similarly, the Xerox technician may have access to the copiers' hard drive to repair the machine, without the covered entity having considered the fact that the drive contains copies of all of the PHI that was copied or printed on that machine.

If an authorized individual during the course of authorized work, permitted by the HIPAA and HITECH rules, has the ability to access more data than they reasonably need to carry out their duties, under the new rules, this fact ALONE would constitute a breach, whether or not the person ever accessed more data than they needed. Moreover, if an employee or agent is exposed to more PHI than they reasonably need, this is a breach irrespective of whether they ever make any other use of that data, disclose it to anyone, or even remember it, and irrespective of whether there is any actual harm to anyone as a result of the "breach." Thus, trivial and inconsequential violations of HIPAA which result in no real "exposure" of patient data may result at least in a breach investigation and remediation, and possibly in a massive breach notification.

Define "Compromised?"

Under the old regime, following the lead of numerous State and Federal data breach notification laws for Personally Identifiable Information (PII), a data breach was the unauthorized acquisition or use of protected data, and a disclosure was required unless there was "no harm." The new OCR rules start with the first part of the definition, but then require the affected entity to conduct an investigation. A breach notification can be avoided only if the investigation demonstrates a low **probability** that the protected health information has been **compromised.**

But neither the statute nor the regulation define what it means to have PHI "compromised." The language of the rule suggests that the term "compromised" is meant to mean "compromised the privacy and/or security" of the information, but any unauthorized access or use of the data constitutes at least a de minimus "compromise" of the PHI. So, by substituting "harm" for "compromise" OCR has muddied the waters.

Burden of Proof and Risk Assessment

Compounding the problem of the expansive definition of "breach" is the fact that the new regulation presumes that a breach HAS occurred. Covered entities and business associates will have the **burden of proof** to demonstrate that all

notifications were provided or that an impermissible use or disclosure did not constitute a breach. But as noted above, if a compromise is equal to a breach, and the entity must demonstrate no compromise, this puts the entity in an impossible position. Therefore, we should assume that the term "compromise" means a violation (breach) which doesn't have a substantial impact.

The new regulation requires both covered entities and their business associates, when confronted with a presumed breach, to conduct a risk assessment of the breach AND to maintain documentation of that risk assessment sufficient to meet the burden of proving that there is a low probability that PHI was compromised.

The rule sets out what it considers to be "objective factors" covered entities and business associates must consider when performing a risk assessment to determine if the protected health information has been compromised and breach notification. These factors include:

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

While a covered entity or business associate may make a notification without (or prior to) conducting the risk assessment, it may not decline to make a breach notification unless it conducts and documents the risk assessment.

Thus, even trivial "breaches" will require a comprehensive and documented risk assessment. While the OCR explains that "[s]ometimes the unauthorized acquisition, access, use, or disclosure of protected health information is so inconsequential that it does not warrant notification" **even these cases have to be investigated**. For example, if a covered entity misdirects a fax containing protected health information to the wrong physician practice, and upon receipt, the receiving physician calls the covered entity to say he has received the fax in error and has destroyed it, under the old rules there would be no reportable "breach" because of the harm rule. Under the new rules, this is presumed to be a reportable breach, and the covered entity now must conduct and document a risk assessment. If the risk assessment concludes that there is a low risk that the PHI has been "compromised" (whatever that means), the covered entity or business associate may avoid a disclosure or notification, but only if this process is documented and the covered entity or business associate meets its burden of proof.

As a practical matter, this means that both covered entities and their business associates will have to have in place a much more formal "breach" notification, investigation, reporting and evaluation process to document not only the investigation, but also how the relevant "risk factors" for breach were considered and evaluated. Remember, the presumption is that a reportable breach occurred.

Risk Factors

The new rules require the risk assessment to consider the impact of four "objective" risk factors in determining whether or not a breach has compromised PHI.

Nature and Extent of PHI

First, the entity must consider the kind of PHI that was "exposed." Is it financial information or other personal information that could be used for identity fraud or identity theft? Financial information could include banking information, credit card numbers, social security numbers, or other information that increases the risk of identity theft or financial fraud and is more likely not only to have been stolen, but also to have been used improperly to the detriment of the data subject. Is the information comprehensive information, or only bits and pieces of a file? Is the information of the type or character that could identify the data subject, or which could result in the re-identification of the information or the subject? A lab report with only values on it may not be sensitive unless it is linked with or could be linked with a specific individual or a small group of individuals.

For clinical or diagnostic information, the entity should consider the nature of the services or other information – the more sensitive the services; the more likely that the information has resulted in a reportable breach, although any clinical information should be considered sensitive. Some clinical data, like diagnosis of teen pregnancy, abortion, sexually transmitted diseases, psychiatric treatment, terminal or genetic diseases or disorders, may be even more sensitive than others. Entities should also consider the amount of detailed clinical information involved (e.g., treatment plan, diagnosis, medication, medical history information, test results). In conducting its risk assessment of "breached" data, the entity should also consider the probability that the protected health information could be used by an unauthorized recipient in a manner adverse to the individual or otherwise used to further the unauthorized recipient's own interests. In other words, "what was 'stolen' and what could someone do with it?"

To Whom Was Information Improperly Disclosed?

The risk assessment must also consider the identity and role of the person or persons to whom there has been an improper disclosure or who made an improper use of the PHI. For example, if PHI is improperly disclosed to a physician, third-party payer, or another entity that has the legal obligations to protect the privacy and security of the information, this may reduce the impact of the improper disclosure. This would be the case if the PHI was impermissibly disclosed to another entity obligated to abide by the HIPAA Privacy and Security Rules or to a Federal agency obligated to comply with the Privacy Act of 1974 and the Federal Information Security Management Act. The same may be true for entities that have other legal or contractual obligations to protect the data – even if they have received it in error. Thus, in the case of the fax misdirected to the wrong doctor's office, the covered entity can rely on the fact that the person receiving the data has a legal obligation to protect it.

In many breach cases however, the entity does not know who had improper or unauthorized access to data. This is particularly true when the "breach" is not a theft of data, but an unauthorized "use" of the data. In the unauthorized "use" cases, the person who used the data in excess of authorization may have been authorized to access the data, and therefore this risk factor may be satisfied. Thus, no single risk factor is determinative of whether a "breach" occurred.

Can the Data Be Re-identified?

One of the issues that entities must consider in determining whether a breach has occurred is whether the data subject to the breach can be re-deidentified. Under the old rule, if the data breached constituted a "limited data set," no breach notice was presumed. Not anymore. Now the presumption is the exact opposite – it is presumed that a breach involving a limited data set is a breach unless, using all of the factors, the entity can demonstrate and document that a breach has not occurred and notification is not required. Presumably the fact that the data breached is a limited data set goes to the issue of nature and extent of PHI breached, and is a factor in mitigation of breach notification, but entities must also consider whether an authorized person with access to a limited data set for one purpose has the ability to re-identify de-identified information or data sets and therefore the ability to use it for an improper purpose. Remember, under the new rules, "breach" includes BOTH unauthorized access or unauthorized use.

Was PHI Actually Acquired or Viewed or Was There Only the Opportunity to Acquire or View the PHI?

Sometimes there is an unauthorized acquisition of hardware or an unauthorized access to a network that contains PHI, but no actual PHI has been compromised. One of the purposes of the mandatory risk assessment is to determine if the protected health information was actually acquired or viewed or, alternatively, if only the opportunity existed for the information to be acquired or viewed. If the information was actually acquired or viewed without authorization or in violation of the HIPAA/HITECH rules, this is more likely to result in a reportable breach. A few examples illustrate this point:

> **Example 1:** A laptop computer containing unsecured PHI is stolen and later recovered. As part of the risk assessment, a forensic analysis shows that the protected health information on the computer was never accessed, viewed, acquired, transferred, or otherwise compromised. As a result of the documented risk assessment, the entity could determine that the information was not actually acquired by an unauthorized individual even though the opportunity existed.

Example 2: A covered entity mails a document containing PHI to the wrong individual who opens the envelope and calls the entity to say that she received the information in error. Under this risk factor, HHS would consider that the unauthorized recipient viewed and acquired the information because she opened and read the information to the extent that she recognized it was mailed to her in error. Thus, according to HHS, this would increase the risk factor's weight.

Example 3. A covered entity mails information containing PHI to a patient's old address, faxes information to the wrong number, leaves a voice message at the wrong number reminding a patient of an upcoming appointment, or, in situations where patients have identical or similar names, contacting the wrong patient to inform him or her that lab results were ready. Again, the entity would have to conduct a documented risk assessment to see whether the information mailed, faxed or left on voicemail was accessed, and whether this constitutes a "breach" of the patient's data.

Note that in each of these cases, there is a slim likelihood that the PHI will be used improperly or for the harm of the patient. Under the old "harm" test, a covered entity could (but not necessarily would) conclude that the fact that the person wrongfully receiving the telephone call, letter, or fax, then called the covered entity or business associate to inform the entity of the mistake, indicates that there is little likelihood that the PHI will be used improperly. Under the new rules however, this is presumptively a reportable data breach. Indeed, if the person who receives the letter or fax improperly throws the paper away after informing the covered entity, this too presumptively becomes a reportable breach, since the paper has now been disposed of improperly!

Are there substantial Mitigating Factors?

Finally, in conducting its own risk assessment, covered entities and their business associates must consider the extent to which the risk to the protected health information has been mitigated. In the case of the misdirected fax or letter, this might be satisfied by obtaining the recipient's satisfactory assurances that the information will not be further used or disclosed (through a confidentiality agreement or similar means) or will be destroyed – and destroyed properly. But the covered entity will have to document the nature and scope of the assurance, and the reasons it believes that these assurances are valid. Do we trust the person, and why or why not? Can we confirm that the information has been deleted? Can we confirm the method or mechanism? Who IS the party with unauthorized access? An employee? An employee of an affiliate? A third-party provider? A stranger?

Consider this example. A "grey-hat" hacker contacts a covered entity's Chief Information Security Officer (CISO) and informs him or her of a discovered vulnerability that would permit access to a network, a portion of which contains PHI. The grey hat assures the CISO that no PHI has been accessed, and asks the CISO to retain the grey hat for assistance in mitigating the vulnerability discovered. A forensic investigation validates the existence of the vulnerability, but log data cannot confirm or deny whether or not the PHI has been accessed by the gray hat hacker. Should the hacker be hired? Should the hacker's assurances be trusted? Do we believe that the PHI has been accessed without authorization or not?

In most risk assessments, the existence or non-existence of mitigating factors will be the difference between a determination of whether information has been compromised (and therefore a breach notification is required) and whether it has not been "compromised" and therefore no notice is required. The ability to conduct and document such a risk assessment, preferably through an independent and trusted third party, may be the difference between having to notify tens of thousands of individuals about a "breach" and being able to simply fix problems or issues as they come up.

Data Protection May Not Be Enough

Another consequence of the presumption of a data breach deals with PHI that is not encrypted, but which is otherwise obscured or protected. Hospitals, providers, payers and others frequently use complicated and archaic data systems for the collection, storage, analysis and transmission of PHI. This may include old mainframe systems, which require special hardware or software, or proprietary networks, operating systems, or software packages. Thus, data (in the form of data tapes, drives, etc.) which may be improperly "accessed" or lost (e.g., lost data tape, lost drive, etc.) may for all practical purposes, be unusable by anyone other than the covered entity or business associate. To reconstruct this data may require millions of dollars of hardware and software, and tens of thousands of man-hours of coding and analysis. For all practical purposes, the lost data is unusable.

Under the new rules however, a breach notification is not required when the PHI is encrypted, not merely obscured. Even if its encrypted, the data breach notification rules are excused only when the PHI is encrypted using methods specified by the Secretary of Health and Human Services in the Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals (74 FR 42740, 42742). Use the wrong method and even if the data is effectively unusable, the new rules presume that there is a reportable breach. The fact that the data is most likely indecipherable becomes just a factor that can be considered in the mandatory risk assessment.

Take Notice

HIPAA and HITECH have long required covered entities to provide their patients with a "Notice of Privacy Practices" which specify what data is being collected, how it is going to be used, and how it will be protected. The new rules may require these notices to be revisited, and may require them to explain how the entity (and/or its business associates) will conduct breach investigations and notifications. Since those affected by a breach may have to notify patients of the circumstances of a breach, as well as what steps individuals should take to protect themselves from potential harm resulting from the breach, some of this information may have to be included in the covered entity's Notice of Privacy Practices.

Knowing What You Don't Know

The HHS final rule triggers a reporting requirement within a certain number of days from when a breach is "discovered." The rule provides two kinds tests for when a breach is "discovered," noting that a breach "shall be treated as discovered by a covered entity on the first day the breach is **known** to the covered entity, or by exercising reasonable diligence would have been known to the covered entity." The regulation defines "reasonable diligence" to mean the "business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances."

So if you know or should have known that a HIPAA violation or misuse of PHI or improper disclosure of PHI has occurred, this triggers the discovery clause.

HHS OCR has indicated that, in determining what a corporate entity "knows" it will apply common-law principles of "agency" – that is, the law of when you are deemed to be responsible for the acts of someone else. And that's where this gets hairy.

Corporate and collective entities are presumed to know what their agents know. So if a low-level health care worker, in the course of their employment, knows there has been a PHI breach or misuse, and fails to tell anyone (say because they have actually been involved in the misuse or breach) the trigger may start when that worker alone "knows" of the breach – not when management knows or should have known. But it may be even worse than that. Corporations or collective entities may be liable for "knowing" something that nobody in the company actually knows because a corporation is presumed to know what every employee and agent knows. So if Employee A knows that there had been a breach into a particular network or computer but doesn't know or have any reason to suspect that that computer contains PHI, but Employee B knows that the computer contains PHI but doesn't know about the breach and believes the PHI to have been encrypted, and Employee C doesn't know that the computer contains PHI or that there has been a breach, but knows that the data on the computer is actually not encrypted, then the corporation as an entity actually knows that there has been a breach of unencrypted PHI even though no employee within the company has this knowledge. And this is actual knowledge, not what the company "should have known." So the time trigger starts immediately. Applying the common law of agency may mean that a company is deemed to know what at least some of its business associates "know" as well, depending on the nature of the work done and the agency relationship. Adding the "should have known" tests means that companies will be required to investigate and report data breaches they don't even know about!

Therefore, HHS OCR has stated that, "We encourage covered entities and business associates to ensure their workforce members and other agents are adequately trained on the importance of prompt reporting of privacy and security incidents." Policy, training, awareness, incident identification, incident reporting and incident response now become critical to avoid fines and penalties.

In addition, the new regulations make it clear that a covered entity is responsible, under the federal common law of agency, for the acts or omissions of its business associates, and that the business associates are liable for the acts of their subcontractors. Thus, companies should revisit the business associate and indemnification agreements to see, at least as between themselves, who is liable for investigating, reporting and paying for a data breach.

Notice of Privacy Practices and Rights to Access Information

The new rules also require both covered entities and their business associates to notify data subjects (patients) of their privacy practices – including their rights to be notified in the event of a data breach. Thus, patients must be told that they have the right to know if their PHI has been misused or accessed without authorization. While this may reflect a minor change, many business associates may have no direct relationship with the patients at all, and therefore have no ability to communicate these privacy practices to the patient. Similarly, the new regulations may be read to give patients (or their family or designees) the right to access their own PHI not only from the covered entity, but potentially from the business associate. As a result, entities that have no relationship with patients directly – law firms, accountants, internet providers, auditors, etc., who may have legitimate access to PHI, may be forced to comply with patient demands for access to PHI, and this duty may not be delegated simply by telling the patient to get the data directly from the covered entity. While a well-crafted business associate agreement may help, this may create record keeping, retention and access issues for business associates.

Take Aways

It is virtually impossible for any covered entity or business associate to completely eliminate the potential that PHI will be either used improperly or disclosed improperly. Therefore, under the new rules, it is critically important that entities that deal with PHI have a comprehensive, robust and documented incident response program, together with a training and awareness program that is reasonable in light of the nature of the institution and the PHI collected or used. The new regulations place a premium on conducting and documenting the incident risk assessment process, and on supporting conclusions about whether a reportable breach has or has not occurred. Having such a program in place can be the difference between having no reportable breach, mitigating the harm from a potential breach beforehand, or having a reportable breach that can cost the institution millions of dollars in damages, fines and lost reputation. A well-tailored security incident response policy, together with the capability of conducting a comprehensive forensic investigation of allegations of data loss will, in both the short term and the long run, ensure compliance with regulation, prevent damage to patient privacy, and inevitably provide better patient outcome by encouraging the responsible flow of PHI to those who need it.

About the Authors

Authored by the CSC Global Cybersecurity Consulting team.

If you have questions or concerns about your organization's ability to meet the new breach rules, or to become and remain compliant with Federal and State regulations, please contact Richard Staynings, Global Coordinator for Healthcare Security at CybersecurityConsulting@csc.com

For a complete listing of CSC Cybersecurity services go to http://www.csc.com/cybersecurity
For a complete listing of CSC Healthcare services go to http://www.csc.com/healthcare

About CSC

The mission of CSC is to be a global leader in providing technology-enabled business solutions and services.

With the broadest range of capabilities, CSC offers clients the solutions they need to manage complexity, focus on core businesses, collaborate with partners and clients, and improve operations.

CSC makes a special point of understanding its clients and provides experts with real-world experience to work with them. CSC is vendor-independent, delivering solutions that best meet each client's unique requirements.

For more than 50 years, clients in industries and governments worldwide have trusted CSC with their business process and information systems outsourcing, systems integration and consulting needs.

The company trades on the New York Stock Exchange under the symbol "CSC."