The Lares Institute

Information Superiority and the Changes to HIPAA
February 2013.

By: Kenneth Mortensen, Andrew Serwin, and Tina Stow.

The Department of Health and Human Services recently released the long-awaited final changes to HIPAA. The Rule makes a number of changes to HIPAA that impact previously covered entities, but one of the more important changes is that businesses that were not in scope of HIPAA can now be considered to be "business associates", and are now subject to many existing requirements, as well as enforcement by the Secretary. In addition, many businesses may be subject to certain obligations as a result of the expansion of coverage for subcontractors, and there is now also a possibility for downstream liability for entities that are not covered entities or business associates, at least in the view of HHS.

These changes place a premium on information governance, as well as data sensitivity, particularly in the data breach context. As such, Information Superiority[1] and Privacy 3.0[2] are doctrines that can help you govern information and optimize your risk.

This White Paper examines the changes for both covered entities, as well as business associates, and notes, where applicable, where existing burdens on covered entities were expanded, or placed upon business associates. This White Paper is based upon an excerpt of the upcoming book "*Health Care Security and Privacy*", which will be published by Thomson-West. More details will be available on January 29, 2013 at http://www.laresinstitute.com/publications and the book is expected to be published by February 15, 2013.

At a top level, the goals of HHS appear to be: enhancing privacy and security protections to prevent a so-called "lapse" in protections for Protected Health Information; applying the Security Rule directly to the activities of business associates; expanding the coverage of HIPAA to business associates; streamlining and simplifying certain existing regulations; increasing enforcement; shifting the regulatory burden regarding subcontractors to business associates; increasing flexibility regarding the use of information for research; placing restrictions on the sale (which could include rental and other forms of sharing) of information, including in situations where there is not financial remuneration; and restricting significantly marketing activities where financial remuneration is received.

Changes to the Definition of Business Associate.

There were a number of changes made to the definition of business associate, which were directed to implement the HITECH Act, make the term consistent with the PSQIA (as patient safety organizations under this law were added to the definition of business associate), and to expand the scope of the definition. Unlike the previously narrower definition of business associate, the definition of a business associate was expanded to cover any entity that creates, receives, maintains, or transmits protected health information for a function or activity regulated by HIPAA, which includes claim processing, or administration, data analytics, processing, or administration, as well as other categories. Health Information Organizations, E-

[1] http://www.laresinstitute.com/information-superiority.
[2] http://www.laresinstitute.com/wp-content/uploads/2012/03/Privacy-3.pdf

prescribing Gateways (in a way HHS believed consistent with the HITECH Act), or other data transmitters, if certain conditions are met (including requiring access on a routine basis to protected health information), are also covered.

In the view of HHS, where a company acts as a "mere conduit" of information, it may not qualify as a business associate, though this is a "fact specific" analysis. The examples provided include the postal service and ISPs, but one could imagine a scenario where an ISP offers services in addition to bandwidth that could alter this conclusion. In the view of HHS, if there is storage of information in a persistent way, or directs the flow of information, even if the company doesn't access the information, the company could be a business associate. Given the addition of the term "data analytics" to the definition of business associates, certain industries that were not directly covered by HIPAA may now have to meet its requirements for business associates.

One other change is that the definition of business associate now includes a subcontractor that creates, receives, maintains, or transmits protected health information on behalf of a business associate. According to HHS commentary, this includes agents of companies that are not under contract, as well as persons who act on behalf of the business associate. The stated goal of this change was to ensure that there was not a gap (a "lapse" as described by HHS) in coverage regarding privacy and security for protected health information merely because the activity in question was performed by a subcontractor. HHS believes clearly this also creates downstream liability for the subcontractors.

The definition of business associate was also amended to include a person that offers a personal health record to one or more individuals on behalf of a covered entity.

While there were some new exclusions added to this definition as well, these changes will likely cause a large expansion of the number of entities that are covered by HIPAA. Many businesses that work with covered entities may now become business associates, and be subject to many of the requirements below, as well as direct enforcement. Moreover, covered entities may be impacted as these changes may increase their need to enter Business Associate Agreements (BAAs) with more vendors and may alter the existing vendor assessment programs of covered entities; however, the good news for covered entities, is that HHS views each level of commerce as having independent liability and contractual privity, which means covered entities do not need to enter into contracts with all levels at which PHI is handled or processed.

Changes to the Definition of Electronic Media.

Additionally, HHS changed the definition of electronic media, to include language changes to conform with NIST Guidance. Amendments were also made to the definition to make clear the view of HHS that Intranets were covered by this definition. There were also some clarifications made related to the definition to illustrate that faxing a hard-copy document, even it is a printed document that was from an electronic file, is not covered.

Enforcement for Business Associates.

Recognizing the expansion of coverage for business associates, the definition of a respondent, which ties to the enforcement power of the Secretary, was expanded to include business associates. Note that this continues through the stream of commerce for the PHI, such that at each level, subcontractors are considered business associates and, thus, are subject to the Secretary's enforcement powers.

Time for Compliance.

The regulation is effective on March 26, 2013, with the time for compliance being September 23, 2013, though the timing in the transition provisions noted below should also be factored in.

Sections 160.306, 160.308, 160.310, and 160.402 Regarding Complaints to the Secretary, Compliance Reviews, Restrictions on Certain Conduct, and Civil Monetary Penalties.

OCR expanded the scope of section 160.306 to include business associates and made other changes regarding the powers of the Secretary to investigate. Similar changes were made to section 160.308 to reflect the expanded scope for business associates.

Section 160.310, which sets certain responsibilities under HIPAA regarding investigations, was similarly expanded to cover business associates, where it had not done so before. The restrictions upon intimidation or coercion for filing complaints were also expanded to cover business associates, as were the basis for civil monetary penalties under 160.402.

Factors for Assessing Civil Monetary Penalties.

The factors the Secretary can consider under Section 160.408 in assessing a civil monetary penalty were modified. This includes changing the mitigating and aggravating factors in assessing civil monetary penalties. The first factor is examining the number of individuals affected and the time period during which the violation occurred. The second factor is the nature and extent of the harm resulting from the violation, which includes whether there was physical harm, whether the violation resulted in financial harm, and whether the violation hindered an individual's ability to obtain healthcare. The old standard regarding the degree of culpability of the covered entity was removed which looked at the intent of the covered entity related to the violation. The remaining sections were amended to include business associates in light of the expansion of the regulations.

For violations where the entity did not know, each violation is $100-$50,000, with a maximum penalty of $1,500,000 for each violation of an identical provision in a calendar year. For violations where the entity acted with reasonable cause, the penalty is $1,000-$50,000 per violation, with the same maximum for all such violations. For cases where the violation was due to willful neglect, but corrected, the penalty is $10,000-$50,000, with the same maximum. For violations where there was willful neglect, and it was not corrected, $10,000-$50,000 with

the same maximum. There is extensive commentary regarding how HHS intends to count these violations, and the maximum violation for each violation might just be the beginning.

Affirmative Defenses and Waiver of Penalties.

The section of the regulations that deals with affirmative defenses was also amended. Some relate to the addition of business associates, and others are changes of dates that relate to whether the alleged act was a violation of other laws, or whether a penalty has already been imposed. There were also changes to the standard regarding whether it would be unreasonable for the covered entity, despite the exercise of ordinary business care and prudence, to comply with the administrative simplification provisions if the violation was not due to willful neglect, subject to other existing limitations. There were also changes to the waiver section regarding civil penalties that alter the Secretary's ability to waive the civil penalties under 160.412.

Changes to the Applicability Language.

Section 164.104(b) was amended to again reinforce the change that business associates were now covered by these regulations, including the HIPAA Privacy, Security, and Breach Notification Rules, though it should be noted that business associates are not subject to all provisions of these Rules, particularly the Privacy Rule. For example, business associates are not required to provide notice of privacy practices, or designate a privacy official, unless this obligation has been delegated by the covered entity. Similarly, a business associate does not have a direct notice of security breach obligation to the individual, in the absence of a delegation. Language was also removed regarding health clearinghouses as it was deemed unnecessary.

Changes Regarding Hybrid Entities—Organizational Requirements.

There were a number of changes made to the regulations regarding hybrid entities, including the removal of a limitation which focused on the requirements of subparts C and E and compliance, so that it would be clear that Parts C, D, and E are relevant, and these changes also carried over into the removal of an explicit reference related to the covered entity ensuring that there was compliance with subparts E and C as part of the safeguard requirements.

Security and Safeguards.

The security standards in 164.306 were also modified to include business associates expressly, with direct liability for violations. There were also certain changes made to the section that addresses maintenance. Section 164.308 regarding administrative safeguards was also updated to cover business associates.

Agreements with Business Associates.

The standard regarding business associate contracts was modified. One new change is that a covered entity is not required to obtain satisfactory assurances from a business associate that is a subcontractor. Instead, business associates are required to obtain satisfactory assurances that the subcontractor will properly safeguard information if the subcontractor is to create, receive, maintain, or transmit electronic protected health information on behalf of the business associate. This directly places the burden regarding subcontractors on the business associate, rather than the covered entity. The HHS commentary makes clear that the covered entity should not contract with the subcontractor, but rather the covered entity must get satisfactory assurances from business associates, and the business associates must, in turn, get the same from their subcontractors. These new requirements will place a premium on vendor assessment, diligence, and contracting for business associates and covered entities.

Certain exceptions to this rule were also removed as part of the amendment, as were certain violations that are applicable to covered entities.

Physical and Technical Safeguards.

Section 164.310 regarding physical safeguards was amended. Business associates are directly covered by these standards for the first time, and there were not significant changes beyond that change in this section. This places certain required and certain addressable requirements upon business associates. The same is true of section 164.312 regarding technical safeguards which is also now directly applicable to business associates.

Organizational Requirements.

The organizational requirements of section 164.314 were amended, and many requirements relate to contracts and other arrangements. The first change was to reflect that the scope of contracts or other arrangements may now go beyond the prior covered entity-business associate relationship. Some of the specific guidance regarding covered entity's compliance, based upon patterns of activity were removed (these were expressed in Section 164.314(a)(1)(i)). Similar changes were made to section (a)(2)(i) as well, and these requirements were "streamlined", based in part upon the existence of parallel requirements in the Privacy Rule.

However, there were additions that place a burden upon business associates to ensure that subcontractors comply with certain obligations in accordance with 164.308(b)(2). As noted above, this is consistent with the placement of the subcontractor's burden on business associates, and not covered entities.

Policies Procedures and Documentation Requirements.

Section 164.316, which addresses policies and procedures and documentation requirements, was expanded to include business associates directly.

Notice of Security Breach.

One area where there were significant changes relates to the notice of security breach standard under HIPAA. HHS believes the changes discussed below clarify that an impermissible use of protected health information is presumed to be a breach unless the business associate or covered entity demonstrates that there is a low probability that the information has been compromised, after a risk analysis is performed. In reviewing the currently known breaches and the comments received on the initial rule, HHS decide to remove the "harm trigger" and rather create liability for every impermissible use or disclosure, HHS instead shifted the analysis (and with that the documentation requirements for recording the decisions surrounding breach notification), and substituted a new risk assessment for the old harm standard. HHS believes this will not materially alter the number of reportable breaches, because of the standards and risk assessment that has been added to the security breach standard. HHS also encouraged companies to take advantage of the encryption safe-harbor.

Looking at the changes directly, a breach is now defined as the "acquisition, access, use, or disclosure of protected health information in a manner not permitted under Subpart E, which compromises the security or privacy of the protected health information". The other exclusions from the definition of a breach that previously existed in what used to be section 2 remained otherwise unchanged. This means that the unintentional acquisition, access, or use of protected health information by workforce member acting under authority is still not a breach if it was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under Subpart E. This is also true for the inadvertent disclosure of information by an authorized person to another person authorized to access protected health information at the same covered entity or business associate. Finally, the exception from the definition of "breach" for unauthorized disclosures where the person receiving the information could not retain it also remained unchanged in the final rule.

The definition of the term "compromises the security or privacy of the protected health information" was removed, as this prior standard was tied to the prior harm trigger, and was limited in certain other ways. A new section was added regarding the risk assessment that is now required. As noted above, the presumption under the statute changed, and acquisition, access, use, or disclosure of protected health information that falls within the definition of breach is presumed to be a breach unless the covered entity or business associate demonstrates that there is a "low probability" that the protected health information has been

compromised based upon a risk assessment. The factors that should be considered in the making of this risk assessment 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.

Although, the HHS commentary seems to indicate otherwise, it could be argued that this new addition appears to at minimum retain, and perhaps strengthen the harm trigger, though it is now couched in terms of a risk assessment. This is particularly true because an assessment of who received the information is permitted, and an express reference to acquisition or viewing was added, as was a mitigation element.

In reviewing the commentary, the first factor requires covered entities and business associates to evaluate the information involved in the potential breach, which includes analyzing the type of information, including whether it is sensitive. HHS offered examples of sensitive financial data, such as: credit card numbers, Social Security numbers; or other information that increases the risk of identity theft or financial fraud. In the case of clinical information HHS stated that this may involve considering not only the nature of the services or other information, but also the amount of detailed clinical information involved. This also includes whether de-identified data could be re-identified, including based upon context.

In addition, research conducted by the Lares Institute sheds further light on this analysis. For example, privacy sensitivity regarding health information varies based upon demographic factors such as age and income, with people in the 46-65 age range being more sensitive than other age groups, and people with higher income being more sensitive about their health information.[3] Also, research done on consumer perception of data sensitivity also can be used in any assessment of information sensitivity.[4]

The second factor focuses on the person who impermissibly used or received information, and part of the analysis includes whether that person has obligations to protect the privacy and security of the information. This also includes a review of whether the information is only impermissibly used within a covered entity or business associate, if there is no further impermissible disclosure outside the entity.

---

[3] *See*, The Demographics of Privacy—A Blueprint for Understanding Consumer Perceptions and Behavior (2011). Certain key statistics are included in Table 1.

[4] *See,* THE EYE OF THE BEHOLDER: OPERATIONALIZING PRIVACY BY DESIGN THROUGH THE POWER OF CONSUMER CHOICE (2012). The list of data elements (including a number of health data elements), ranked by sensitivity, are included in Table 2.

The third factor examines whether information was actually acquired or viewed. This could involve a forensic analysis of electronic information to prove that information was not acquired, and this analysis is similar to the state law analysis that occurs in most breaches. In one example from the HHS commentary, a letter, although incorrectly address, but returned unopened would be leaning toward a "low risk" of compromise (although the commentary indicate if a letter is opened, it could not be low, which seems to overshadow all the other factors).

The final factor considers what mitigation steps have been taken, including obtaining satisfactory assurances from the recipient that the information will not be further used or disclosed, or the information will be destroyed. HHS notes that in its opinion the analysis of the importance of confidentiality or destruction as a mitigating factor may depend on whether a third-party was involved.

In the final analysis, these factors, plus other factors, may also be considered and HHS stated that it expects the risk assessments to be thorough, completed in good faith, with reasonable conclusion. Overall, while the presumption shifted, and the risk analysis may require some additional documentation and investigation of potential breaches, the actual notice obligation may not have expanded. Furthermore, organizations should not give each factor equal weight in every situation, as the examples from HHS clearly indicated that certain scenarios could require particular factors be given more weight.

As shown by the research regarding data breaches done by The Lares Institute, in many cases, particularly where the main potential harm is financial, there may not be risk sufficient to trigger notice in a significant number of breaches.[5]

Prior changes in the Interim Final Rule regarding notification to the media in section 164.406, notification to the Secretary under 164.408, as well as notification by business associate under 164.410 were retained in the Final Rule.

Administrative Requirements and Burden of Proof.

These standards were modified as part of the Interim Final Rule, but it is worth noting that in the commentary, HHS stated that these changes place a burden upon covered entities and business associates to, following an impermissible use or disclosure under the Privacy Rule, demonstrate that all required notifications were made, as well as demonstrate that the use or disclosure was not a breach, if applicable.

Applicability of Section 164.500.

Section 164.500 was amended to add a new sub-section that makes clear that, where provided, the standards, requirements, and implementation specifications of the subpart apply to

[5] See, Data Breaches and the Phantom Damage Allegation, (2011).

business associates with respect to the protected health information of the covered entity. The definition of healthcare operations was also amended to include patient safety activities and a new exception related to the standards under 164.502 (a)(5)(i) regarding health insurance was also added.

In what is one of the more important changes, the definition of marketing was changed in certain ways that could restrict marketing activities under HIPAA. The exclusions from marketing are now limited in a way that could be read to prohibit many communications that currently occur, because HIPAA previously permitted certain marketing communications without regard to whether financial remuneration was received. Under the new definition, if financial remuneration is received, it appears that certain communications will be considered marketing, and therefore restricted or prohibited in some cases.

A definition of "financial remuneration" was added, and is defined as "direct *or indirect* payment from or on behalf of a third party whose product or service is being described." (italics added). There are exceptions to this definition, including payment for treatment of an individual. It should also be noted that HHS believes that these restrictions apply even where the business associate, including a subcontractor, as opposed to the covered entity, receives the financial remuneration for making a communication. HHS also believes that subsidized communications fall within this definition.

However, HHS has stated that it does not believe that financial remuneration includes "in-kind" benefits, and it does not apply to financial remuneration for a purpose other than making the communication, which may provide some flexibility for covered entities.

New examples of permitted communications that are not prohibited include refill reminders and other communications related to biologics or drugs that are currently prescribed for an individual, with certain limitations, as well as for certain treatment and health care operations purposes, unless the covered entity receives financial remuneration in exchange for making the communication. The pre-existing exception for treatment of an individual by healthcare provider including for case management to describe health-related products or service that is provided by or included in the plan of benefits remained, and a new section regarding case management or care coordination was added.

Overall, marketing has been restricted, but as noted below, the restrictions on the sale of information are likely even broader.

Use and Disclosures of Protected Health Information.

Consistent with other changes, business associates were added to the coverage of section 164.502, which regulates the use and disclosure of protected health information. The rules for covered entities did not change, but two new sections related to the obligations of business associates were added.

Section 164.502(3) sets the rules regarding permitted uses and disclosures for business associates, and it includes a limitation that states that protected health information can only be used as permitted by the contract or other arrangement with the covered entity, or required by law. It also restricts business associates from using or disclosing protected health information in a manner that would violate the requirements of this subpart of HIPAA, with certain limited exceptions. There are also required disclosures that must be made by business associates, including disclosures to the Secretary to investigate compliance with HIPAA, and disclosures to the covered entity, individual, or individual's designee, as necessary to satisfy a covered entity's obligations under section 164.524(c)(2)(ii) and (3)(ii) with respect to a request for an electronic copy of protected health information.

Sale of Protected Health Information and Minimum Necessary.

Consistent with the restrictions upon marketing, a new section that addresses the sale of protected health information was added. This places restrictions on the sale of protected health information by both covered entities and business associates. The term "sale of protected health information" is defined to be, except as otherwise provided, a disclosure where the covered entity or business associate directly or indirectly receives remuneration from or on behalf of the recipient of the protected health information in exchange for the protected health information. The exceptions to this definition include disclosures:

- for public health purposes pursuant to section 164.512(b) or 164.514(e);
- for research purposes pursuant to other sections of HIPAA where the only remuneration received is a reasonable cost-based fee to cover the cost to prepare and transmit the information;
- for treatment and payment purposes pursuant to other statutory requirements;
- as part of the sale, transfer, merger, or consolidation of all or part of a covered entity and for related due diligence (which also relates to the definition of healthcare operations);
- to or by a business associate for activities that the business associate undertakes on behalf of a covered entity, or on behalf of a business associate in the case of a subcontractor where the only remuneration that is received is for the services provided;
- to an individual pursuant to other sections of HIPAA;
- as required by law in certain circumstances; and
- for certain other purposes consistent with HIPAA.

One question that these changes raise relates to the sale of a business associate, and related due diligence, because those disclosures are not expressly covered in the new section dealing with the due diligence and sale of a covered entity.

While this provision works in conjunction with the marketing restrictions, it is being interpreted differently than the marketing restrictions in certain ways. First, it should be noted that the restrictions on "sales" are believed by HHS to apply to disclosures in exchange for remuneration that are the result of "access, license, or lease agreements", and unlike the restrictions on marketing, HHS believes that the restrictions on sale of information apply even to in-kind remuneration, and are not limited to financial remuneration.

HHS also attempted to clarify, in response to comments, that uses of protected health information within a single legal entity are not implicated by the remuneration prohibition. This is also true where there are separate legal covered entities that are under common ownership or control if they have designated themselves as an affiliated covered entity.

The minimum necessary standard expressed in this section was also amended to expressly include business associates.

Satisfactory Assurances and Decedent's Information.

The standard regarding disclosures to business associates were modified including expanding the first section regarding satisfactory assurances. Moreover it was expressly stated in the regulations that a covered entity is not required to obtain satisfactory assurances from a business associate that is a subcontractor. A new section was added that covers a business associate's disclosures to subcontractors, and the section requires that the business associate get satisfactory assurances from a subcontractor that the subcontractor will appropriately safeguard information. Certain more specific sections were removed from the standard, and the standards regarding deceased individuals were also modified in that they were limited to cover deceased individuals for 50 years following their death.

Organizational Requirements.

The restrictions regarding uses and disclosures were changed regarding termination of contracts or arrangements, because the requirements regarding what to do if termination is not possible were changed. Moreover, a new section that defines compliance with these standards, including the standards of 164.502(e), was added and it relates to the obligations that are imposed when a pattern of activity or practices by a subcontractor constitutes a material breach or violation of the agreement. There were also additional changes made regarding the obligations of business associates where the business associate is carrying out a covered entity's obligations under this subpart.

An additional section was added that permits a covered entity to comply with this requirement if it discloses only a limited data set to a business associate so that the business associate can carry out healthcare operations functions, and an agreement is in place that complies with the applicable requirements.

There are also some additional requirements regarding business associate contracts with subcontractors.

Uses and Disclosures for Treatment, Payment or Health Care Operations.

Some changes were made to 164.506 regarding permitted uses and disclosures that appear to expand the ability to disclose, because disclosures are no longer limited to other covered entities that participate in an organized health care arrangement.

Uses and Disclosures for which Authorization is Required.

The requirements regarding disclosures under authorization were changed, including regarding marketing. A new section was also added to address the sale of protected health information which requires a covered entity to obtain an authorization for any disclosure of protected health information which is a "sale" as defined under section 164.501. An authorization used for these purposes must state that the disclosure will result in remuneration of a covered entity.

The method of obtaining authorization for the use and disclosure of protected health information for research studies was amended in ways that permit the authorization to be combined with other requests, which is a so-called compound authorization. There are also requirements related to the ability of a covered entity to condition providing research-related treatment on obtaining authorization for the use or disclosure protected health information for research.

Genetic Information.

There were also new sections added regarding the use of genetic information, and definitions that generally track GINA were also added. The definition of health information was also expanded to include genetic information. The rules regarding the disclosure of genetic information that were added include restrictions on the use of genetic information for underwriting purposes by health plans.

Uses and Disclosures Requiring an Opportunity to Agree or to Object.

Section 164.510, which relates to uses and disclosures requiring an opportunity for the individual to agree or object, was also modified in slight ways regarding the requirements and disclosures for directory information. There were modifications to the ability of a covered entity to disclose certain information to a family member, other relative, or close personal friend of the individual, which include uses and disclosures when the individual is not present, and certain uses and disclosures when the individual is deceased.

Uses and Disclosures for Which an Authorization or Opportunity to Agree or to Object is Not Required.

Section 164.512 was modified to clarify that both uses and disclosures were covered, and a section related to disclosures to employers was also expanded by the removal of a section that tied disclosure to the covered entity being a member of the workforce of the employer. There were new exceptions added regarding disclosures to schools in certain circumstances.

Other Requirements Relating to Uses and Disclosures of Protected Health Information.

Section 164.514 was modified in a variety of ways, including regarding uses and disclosures for fundraising. This includes an expansion of how demographic information is defined for fundraising purposes, as the amended language now explicitly includes name, address, other contact information, age, gender, and date of birth. Moreover, additional information including department of service information, treating physician, outcome information, and health insurance status can also be disclosed for these purposes.

There is also now a requirement that each fundraising communication give the recipient clear and conspicuous opportunities to elect not to receive further fundraising communications, and the opt-out method provided must not cause the individual to incur undue burden or more than a nominal cost. Requirements that make explicit a covered entity's obligation not to condition treatment or payment on the individual's choice with respect to these communications was also added, as was the explicit statement that an opt-out must be honored, and a recognition that a covered entity could provide an individual who has opted-out the right to opt back in.

Notice of Privacy Practices.

The requirements regarding notice of privacy practices for protected health information were also modified in certain ways. Specifically, the requirements regarding the contents of the notice were changed to require the inclusion of a description of the types of uses and disclosures that require an authorization under 164.508(a)(2)-(a)(4). There was also a change that requires language to be added in the notice stating that disclosures that are not contemplated in the notice will only be made with written authorization, and that the authorization can be revoked. Furthermore, HHS wants organizations to make clear what rights an individual would have in the case of a data breach and what sorts of mitigating actions the organization will take in the case of a data breach, as well as reference the notice obligation.

The commentary by HHS indicates that it does not believe that all situations requiring authorization be included in the notice. Instead, HHS believes that the notice should, at minimum, contain a statement regarding psychotherapy notes (where appropriate), uses and disclosures of protected health information for marketing purposes, and disclosures that constitute a sale of protected health information require authorization, in addition to the statement that uses and disclosures other than those in the notice will be made only with

authorization. HHS believes that notice of the right to opt-out of fundraising be included as well, as well as the other new rights to restrict certain disclosures.

The requirements regarding separate statements for certain uses or disclosures were also modified. The prior regulation required that a separate statement be included related to contacting an individual to provide appointment reminders or information about treatment alternatives, and this requirement was removed. Moreover, certain other statutory changes that have been previously discussed were also reflected in this section. A new requirement for health plans related to genetic information was also added.

There were modifications to the requirements for health plans, and one of the requirements related to material revisions of the notice was removed, but added as amended in a later portion of the regulation. The other changes largely relate to some additional language related to posting of notices on websites. There is also a change that requires health plans that perform underwriting to include statements regarding the prohibitions on the use and disclosure of genetic information.

The final rule also requires organizations to inform individuals of the new right to restrict certain disclosures of protected health information to a health plan where the individual pays out of pocket in full for the health care item or service. Only health care providers are required to include such a statement in the Notice and other covered entities may retain the existing language indicating that a covered entity is not required to agree to a requested restriction.

In addition to the more organizational components of the Notice, HHS also believes that providing specific reference to how an individual would receive notice of the right of affected individuals to be notified following a breach of unsecured protected health information. This should make clear the obligations of covered entities to provide notification following a data breach. HHS does not believe that this will cause individuals unnecessary concern and unfounded fear that covered entities cannot appropriately secure protected health information, but rather give individuals a useful context should those individuals later receive a breach notification. A simple statement in the Notice that an individual has a right to or will receive notifications of data breaches of unsecured protected health information will suffice and HHS is not looking for a complex solution under the Notice requirement and, as such, the statement need not be specific, such as by describing how a risk assessment will be conducted, include the regulatory descriptions of “breach” or “unsecured PHI,” or describe the types of information to be provided in the actual breach notification to the individual. Nevertheless, organizations may wish considering to provide more than a minimal amount of information.

As noted above, this section contains requirements that apply to covered entities, not business associates. HHS believes these changes constitute material changes, which will likely require covered entities to give notices to individuals that are compliant with the new standards. This may not require providing it directly to each individual, and instead clear and prominent posting, along with having copies of the notice available, would appear to comply with the requirements. The posting may be a summary, as long as the full notice is available in close

proximity. Providers are, at this time, according to HHS, only required to give a copy of a notice with the new disclosures to new patients, and obtain a good faith acknowledgement.

HHS also noted that portions of the ADA and the Rehabilitation Act might impact the format in which the notice is provided.

Rights to Request Privacy Protection for Protected Health Information.

The rights of an individual to request privacy protection for protected health information were also modified. Previously, a covered entity was not required to agree with a restriction, but this right was modified somewhat through the addition of a new section that requires a covered entity to agree to restrict disclosure of protected health information about the individual to a health plan if: the disclosure is for the purpose of carrying a payment or health care operations and is not otherwise required by law; and the protected health information pertains solely to a health care item or service for which the individual, or person other than the health plan on behalf of individual, has paid a covered entity in full. The requirements regarding termination of a restriction were also amended to reflect these changes.

Access of Individuals to Protected Health Information.

Section 164.524 was modified in that the section that addressed protected health information that was not maintained or accessible to the covered entity on site was removed. Additional changes were made regarding the form of access required in the case of electronic information, and these requirements mandate certain forms of disclosures if electronic information is requested, and the information is stored in electronic form. Specific requirements regarding disclosure to another person designated by the individual were also added, and it should be noted that an individual's request to disclose to another must be in writing, signed by the individual, and clearly identify the designated person. The recoverable costs for copying were also slightly amended.

Administrative Requirements.

The administrative requirements under 164.530 were also previously amended by the Interim Final Rule.

Transition Provisions.

The transition provisions address the effect of prior waivers and authorizations. Moreover, there were changes made to deemed compliance for contracts and documentation which reflect coverage of business associates relationships with subcontractors, including regarding contracts that were entered prior to January 25, 2013, if the contract complies with the applicable provisions that were in effect on the date it was entered, and the contract or other arrangement is not reviewed or modified from March 26, 2013 to September 23, 2013. If this standard is met, the deemed compliance period runs until the earlier of: the date the contract

or other arrangement is renewed or modified on or after September 23, 2013; or September 22, 2014. There were additional sections added to address prior data use agreements where limited data sets were disclosed in exchange for remuneration, and these agreements are subject to the same time requirements discussed above.

Costs and Benefits.

Two other notable issues are: the overall cost estimate that was given by HHS; as well as the discussions of benefits of the Rule. HHS provided a cost estimate for the implementation of the Rule, which it estimated to be between $114 million and $225.4 million in the first year of implementation, and approximately $14.5 million thereafter. The cost estimate purports to include: costs to HIPAA covered entities of revising and distributing new notices of privacy practices; costs to covered entities related to compliance with breach notification requirements; costs for certain business associates to bring subcontractors into compliance; and costs to certain business associates to achieve full compliance with the Security Rule. This seems to be a fairly low and, perhaps, unreasonable cost estimate given the breadth of the changes in the Rules. For example, just addressing the need for covered entities to release a new Notice of Privacy Practices could cost at least $250 million.[6]

Notably, HHS stated it could not quantify the "benefits" of the Rule because of a lack of data and the "impossibility of monetizing the value of individuals' privacy and dignity," expanded rights, and also improved enforcement. HHS also believed that the Rule could result in cost savings to companies as well.

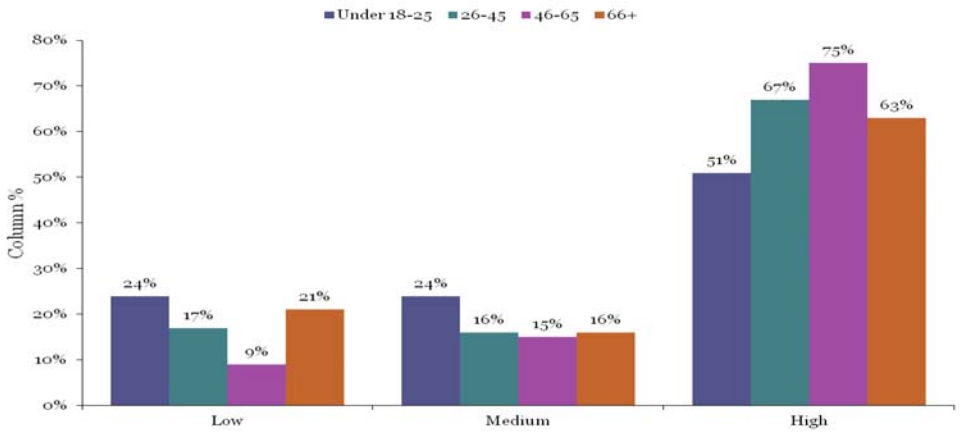
[6] From the Census Bureau Report, Health Status, Health Insurance, and Medical Services Utilization: 2010. In 2010, there were 304,814,000 individuals in the U.S. of which 82.6% had insurance, which means they were likely to have interactions with a primary care physician, their health plan, and a pharmacy and (in some cases) dentist or opthamologist, each of which would need to provide a 'new' notice of privacy practices. Assuming a factor of 3.25 for the number of covered entities involved, because although likely that everyone will have the first three, not as likely they will have the fourth, and assuming a cost of $0.33 per notice provided (which is likely low, since paper copies would need to be available), the cost for just notices under the rule is $270 million.

Table 1.

This data comes from the Lares Institute White Paper:

[The Demographics of Privacy—A Blueprint for Understanding Consumer Perceptions and Behavior.]

Health Privacy Sensitivity: By Age.



Privacy Sensitivity: By Income.

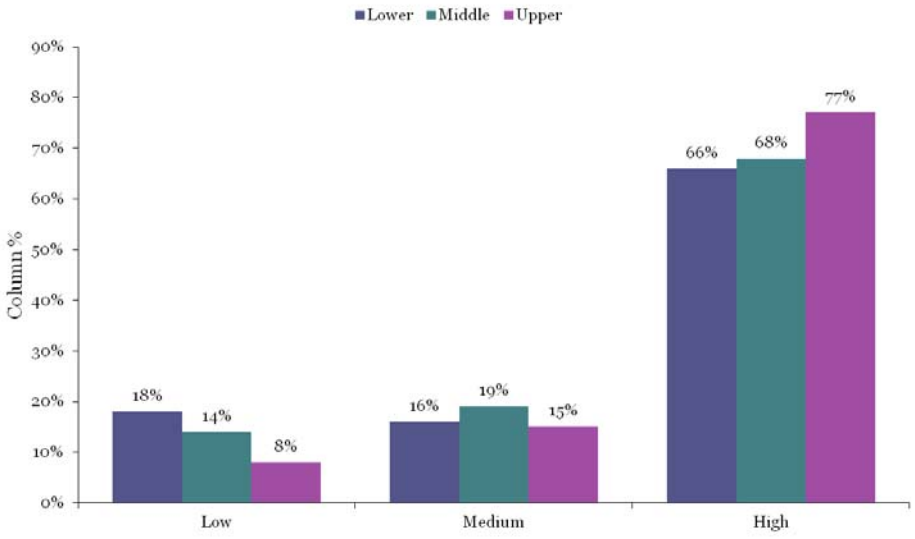


Table 2.

This data comes from the Lares Institute White Paper:

THE EYE OF THE BEHOLDER: OPERATIONALIZING PRIVACY BY DESIGN THROUGH THE POWER OF CONSUMER CHOICE

Quartile 1.

- Social Security number.
- Password or other personal identification number required to access an account or services.
- Credit card or other account number, including information associated with a credit card.
- Financial information, including income tax filings, and financial statements.
- Any ID or number assigned to an individual, including account numbers, user IDs, or passwords.
- Payment card information (debit or credit card).
- Account balances.
- Automated or electronic signatures.
- Information from the computer chip, magnetic strip of a credit or other payment card.
- Alien registration number, government passport number, employer identification number, taxpayer identification number, Medicaid account number, food stamp account number, medical identification number or health insurance identification number.
- Information regarding credit standing or worthiness, assets, or liabilities including a person's credit capacity, character, general reputation, personal characteristics, or mode of living.
- Answers to security questions (for dual authentication purposes).
- Information regarding a home security system.

- Biometric information or numerical representation of biometric data, including finger/voice prints, handwriting, etc.
- Health plan beneficiary numbers.
- Information regarding income or other related information.
- Employee account information.
- Information regarding health insurance, including the existence of insurance or claims history.
- The content of electronic communications such as texts or emails.
- Employee ID.
- Employment evaluations, including information regarding disciplinary actions.
- Physician/laboratory test orders.
- Health insurance application information.
- Information regarding past, present, or future health or conditions, including information regarding medical treatment.
- Information collected from the respondent's children.

Quartile 2.

- Information regarding insurance or insurance claim history.
- Serial numbers for any mobile device (cell phone or PDA).
- Background check information.
- Any ID assigned to a respondent by a non-governmental agency.
- A Persistent Identifier, such as a customer number, that is combined with other identifiable information about the respondent.
- The identities of people respondents emailed or called.
- Voided checks.
- Information regarding prescription drugs taken by respondents.
- Prescription history.

- Location-based information.
- IP Address.
- Cell or mobile device number, including unique device identifier (UDID) for a mobile device.
- Information regarding specific diseases a respondent might have.
- Personally Identifiable Dates, such as date of birth.
- Payment history for any services or products.
- Information regarding a government ID other than a driver's license.
- Government clearance information.
- Age or gender of children.
- Overdraft history.
- Information regarding non-financial accounts, including any house or similar accounts.
- Diagnostic images, such as x-rays, MRIs, or CAT scans.
- Purchase history at a drug store.
- Information regarding an application for homeowner's insurance.
- Any information on a phone bill.
- Information regarding employment.

Quartile 3.

- Information from medical devices.
- Vehicle identifiers and serial numbers, including license plates.
- Information regarding a respondent's residence other than address.
- Family health history.
- Information regarding participation in clinical trials.
- Arrest records.

- Mother's Maiden name.
- Information regarding drug use or addictions.
- Drug testing information.
- Home address.
- Purchase history regarding online purchases.
- Information regarding searches on the Internet.
- Genetic information.
- Audio recordings of a respondent.
- Student identification.
- Telephone number.
- Photographs or videos of a respondent.
- A history of websites a respondent visited.
- Information regarding where a respondent has traveled, including airline records.
- Information regarding use of social networking services.
- Student records.
- Email address.
- The number of any professional, occupational, recreational or governmental license, certificate, permit or membership a respondent has.
- Information regarding a government-sanctioned professional license, or other professional certification number.
- Current or former name.

Quartile 4.

- Information regarding criminal convictions.
- Instant message identifier.
- Information pertaining to service in the Armed Forces.

- Information regarding professional or employment history.
- Fax number.
- Information that reveals what hotels a respondent has stayed at.
- Place of birth.
- Information regarding sexual orientation.
- Purchase history of products or services.
- Information regarding use of apps, games, or other similar information.
- Grades from college.
- Information that reveals utility usage.
- Purchase history regarding purchases of books.
- Diet or exercise-related information.
- Information regarding your ethnicity, nationality, or citizenship.
- Information regarding marital status.
- Occupation.
- Purchase history regarding a respondent's viewing of movies.
- Information regarding philosophical beliefs.
- Information regarding political beliefs.
- Educational history.
- What a respondent "likes" on Facebook.
- Information regarding religious beliefs.
- Information regarding games played online.
- Television viewing information.