HITECH Privacy, Security, Enforcement, Breach & GINA—The Final Omnibus Rule Frequently Asked Questions and Answers

Disclaimer: The following questions and answers are not legal advice or opinion. They are for guidance purposes only. Please seek legal counsel and the law itself for further clarification and understanding.

General Questions

- **When do the new rules become effective?**

  Effective date: March 26, 2013
  Compliance Date: September 23, 2013

- **Where can I download the full text version of the HIPAA privacy and security rule on the web?**

  The final Omnibus Rule is available at http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf. However, the changes likely will not be incorporated into the HIPAA regulations in the Code of Federal Regulations until the October 2013 update.

- **Does AHIMA have an analysis available summarizing the Omnibus Rule?**

  Yes. The analysis is available online at:
  http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_050067.pdf

Business Associate (BA) Questions:

- **Do Business Associate Agreements (BAAs) need to be updated to meet compliance with the Omnibus Rule?**

  Yes, BAAs must be updated to meet compliance with the Omnibus Rule. The dates vary depending upon when the original contract was signed or became effective.

- **When must BAAs be updated by?**

  If you have a HIPAA compliant agreement in place prior to January 25, 2013, and if it is not due to be renewed by September 23, 2013, then the parties have until September 23, 2014 to revise the agreement. In contrast, if the covered entity or business associate executed the agreement on or after January 25, 2013, then the parties will want to either ensure that it complies with the new rule or plan on revising the agreement in 2013, no later than September 23, 2013, to bring the agreement into compliance with the new rule.

  If an agreement is renewed between Sept. 23, 2013 and Sept. 23, 2014, it must comply with the new Omnibus rule.

- **Do we need a BAA for our hospital's foundation?**

  A covered entity may use or disclose to a business associate or to an institutionally related foundation the following protected health information for the purpose of raising funds for its own benefit, without an authorization meeting the requirements of HIPAA § 164.508:
  - Demographic information relating to an individual, including name, address, other contact information, age, gender, and date of birth
  - Dates of healthcare provided to an individual
  - Department of service information
  - Treating physician
  - Outcome information
  - Health insurance status

  A covered entity must include the required statement for fundraising in its notice of privacy practices stating that protected health information (PHI) may be used for fundraising.

- **If the hospital has a BAA with a company and that company subcontracts, does the hospital need to have a copy of the subcontractor's BAA on file?**

  No. The final rule expressly provides that a covered entity is not required to enter into a business associate agreement with a business associate that is a subcontractor. Rather, this is the obligation of the business associate that has engaged the subcontractor to perform a function or service that involves the use or disclosure of PHI.

- **A covered entity is required to have a BAA with its business associates, but does a business associate have an affirmative duty to ensure a BAA is in place with the covered entities with which it contracts?**

  No, nothing in HIPAA requires a business associate to obtain a business associate agreement with the covered entity. Rather, the obligation rests with the covered entity. However, even in the absence of such an agreement, the business associate remains directly liable under HIPAA for certain privacy and security provisions.

- **Are business associates only responsible for reporting breaches to the covered entity's they perform services to, or must they also report to the Department of Health and Human Services (HHS)? For example, if the business associate of a covered entity (i.e., hospital or physician practice) breaches the data, who has the responsibility of breach notification—the covered entity or the business associate?**

  Section 164.404 – 164.410 A subcontractor reports the breach to the business associate, the business associate reports the breach to the covered entity and the covered entity reports the breach to the affected individuals, the Secretary of the Department of Health and Human Services, and, if applicable, the media,, unless it has delegated such responsibilities to a business associate.

- **If a covered entity (i.e., physician practice) contracts out their billing services and wants the billing company to have direct access to the hospital's information system, would the hospital treat the billing company as a subcontractor or business associate?**

Possibly neither. This will be very fact specific, but if the community physicians are not employees of the hospital, then the billing company may be a business associate solely of the community physicians. The hospital may be permitted to provide access to the billing company as a disclosure to another covered entity's business associate for the other covered entity's payment purposes.

Immunizations

- **The sexually transmitted disease HPV can be included in a minor's protected health information. Does the HIPAA change, which permits the release of immunizations with a verbal agreement, exclude releasing HPV vaccinations?**

  Only where states require immunizations for admittance to schools may immunization information be released. Only the immunizations required by that state for individuals to be admitted to a school should be released.

- **Do you still have to account for the disclosure of immunization information as a non-compliant authorization?**

  Actually, you did not need to account for the disclosure before, meaning you did not need to include it in an accounting of disclosures, but will need to do so now due to the change in the law. Previously in all cases, an authorization was required for disclosure of immunizations to schools. The change in the law now permits release with a verbal agreement. The accounting of disclosures provision accepts disclosures pursuant to an authorization. Now, if certain criteria are met, no authorization is required to disclose student immunization records to a school. The disclosure, which is treated as a disclosure for a public health activity, would no longer fall under an exception to the accounting of disclosures rule and, therefore, would need to be included in an accounting of disclosures. The disclosure would also be subject to accounting under the proposed modifications to the accounting of disclosures provision, since public health disclosures remain subject to accounting.

  For immunization, it requires agreement, but not an "authorization" (which, though not defined, is a term under HIPAA referencing the document set forth at 164.508). So prior disclosures of immunization records were "pursuant to an authorization as provided in § 164.508" and therefore were exempted from accounting. But disclosures that fit under the new exception will not be pursuant to an authorization provided for in 164.508. Rather, they will fall under the public health permission at 164.512(b).

Breaches:

- **Protected health information was faxed to the wrong nursing home. The recipient of the fax was a covered entity. Is this a breach?**

  In this case the recipient has obligations to protect the privacy and security of the disclosed information. It will take some investigation to determine if the information was viewed at the receiving entity or if their staff received the fax and immediately determined it was in error and returned or destroyed the information. But, this scenario may not be a breach.

- **Someone on our staff lost a flash drive containing protected health information. The drive was encrypted. Is this a breach?**

  No. The data must be unsecured to meet the definition of a breach. HHS issued guidance on how to render PHI unusable, unreadable, and indecipherable. If PHI has not been rendered secure in accordance with the specified guidance and a violation has occurred, then it must be presumed to be a breach. This guidance can be found at: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html.

- **As a health information consultant and a business associate to the covered entity, chart audits are performed taking notes of deficient documentation items. These worksheets include various types of information (i.e., room number and patient initials to ID the patient on confidential worksheets used by the administrative staff). If this information is on a mobile device (i.e., laptop) and the laptop was stolen, will this be considered a reportable breach? How do you calculate a risk assessment if the information is lost or stolen? How can one assess if the information has been viewed or used in any way?**

  First, was the PHI on the laptop encrypted? If yes, then no further action for handling a breach is required.

  If no, then there appears to be a reasonable argument that the information was not compromised if the only identifiers included room number, patient initials, and relevant dates, since there is a low probability that the thief would have the resources or motivation to identify the information. There is some risk, though, since the new compromise standard is subject to interpretation.

- **What should I do if information is breached during a disaster?**

  Contact the regional and national Office for Civil Rights (OCR) to inquire about a HIPAA waiver and its use in your particular situation. If PHI is breached, work with legal counsel to notify OCR, accrediting agencies such as the Joint Commission, and business partners. Ask OCR for clarification on handling records and inquire if press coverage will satisfy the greater than 500 (affected individuals) provision of the breach notification rule. For more information, visit HHS' guidance on Disclosures in Emergency Situations.

Decedents:

- **Regarding decedent information, if state law says that a personal representative is required to be given access to a patient's records, do we follow state law assuming preemption applies and the most stringent law takes precedence (i.e., state law that is more restrictive)?**

  Yes, the law that gives greater protection to the patient is the one that takes precedence. If a state law prohibits disclosing to anyone other than the personal representative, then that state law would continue to apply. If the state law indicates who is the personal representative but does not limit disclosure to others, then the covered entity may disclose to persons who were

involved in care or payment and are not the personal representative, if the information is relevant to their involvement (i.e., relates to the episode of care) and the decedent had not expressed contrary wishes.

- **If an individual, prior to death, expresses a preference to not release any information to a personal representative, family or friend, how is the covered entity to document this?**

  This is an operational question that one must implement at their specific facility. The Privacy Rule does not direct the industry how to document the information, only requires that facilities do document it and then honor the request.
  Note: A personal representative generally has a right to access the decedent's information, regardless of the decedent's wishes. So, if an individual expresses this preference prior to death, the individual should have any legal documentation updated to reflect that change.

- **How is the term "involved in the decedents care or payment" defined?**

  The rule is not prescriptive. The preamble states:
  "This will ensure family members and others can find out about the circumstances surrounding the death of their loved ones, unless the individual prior to his or her death objected to the covered entity making such communications. Further, the Privacy Rule limits such disclosures, similar to the other disclosures permitted under § 164.510(b), to the protected health information relevant to the family member or other person's involvement in the individual's healthcare or payment for healthcare. For example, a covered healthcare provider could describe the circumstances that led to an individual's passing with the decedent's sister who is asking about her sibling's death. In addition, a covered healthcare provider could disclose billing information to a family member of a decedent who is assisting with wrapping up the decedent's estate. However, in both of these cases, the provider generally should not share information about past, unrelated medical problems. Finally, these disclosures are permitted and not required, and thus, a covered entity that questions the relationship of the person to the decedent or otherwise believes, based on the circumstances, that disclosure of the decedent's protected health information would not be appropriate is not required to make the disclosure."

Electronic Access

- **Does the charge for labor and electronic media pertain to other parties than the patient, such as lawyers?**

  If the request is coming from the patient (or personal representative), then arguably charges are limited regardless of who is the recipient. It does not matter who pays the charges. If the request is coming from a third party, such as a lawyer, then a patient authorization is required (unless another HIPAA permission applies, such as a subpoena) and there is no limit on charges under HIPAA (there could be limits under state law).

- **What can be included as part of billable labor costs when determining fees for record requests?**

This provision allows for identifying the labor for copying protected health information, whether in paper or electronic form. Labor costs can include a reasonable cost-based fee for skilled technical staff time spent creating and copying electronic files and doing work like:

- compiling
- extracting
- scanning
- burning onto media
- distributing media

This could also include the time spend preparing an explanation or summary.
Other fees include:

- cost of supplies for creating the paper copy or electronic media (if the individual requests portable media)
- postage or courier

This provision clarifies that a covered entity may not charge for a retrieval fee, whether it is a standard retrieval fee or one based on actual retrieval costs.

- **The cost of copying health information is set by state law, which is used by the copy service. How do we determine cost per page taking into account state law?**

The Omnibus preamble explicitly states that covered entities need to determine if the fee is reasonable. When a state law provides a limit on the fee that a covered entity may charge for a copy of protected health information, this is relevant in determining whether a covered entity's fee is ''reasonable''. A covered entity's fee must be both *reasonable* and *cost-based*. For example, if a state permits a charge of 25 cents per page, but a covered entity is able to provide an electronic copy at a cost of 5 cents per page, then the covered entity may not charge more than 5 cents per page (since that is the reasonable and cost-based amount). Similarly, if a covered entity's cost is 30 cents per page but the state law limits the covered entity's charge to 25 cents per page, then the covered entity may not charge more than 25 cents per page (since charging 30 cents per page would be the cost-based amount, but would not be reasonable in light of the state law).

- **Does a covered entity or business associate have to release existing paper records in electronic media, if requested? Would the charge then be by page count or electronic media?**

An entity has to provide the copy in the form and format requested, if readily producible. There is a lack of clarity, though, on what is meant by "readily producible." The preamble does indicate that you are not required to scan paper documents to provide electronic copies. Accordingly, providing paper copies remains permissible. There is nothing to preclude you from agreeing to scan the documents and convert them into electronic media. It may be best to inform the individual of the potential costs of scanning and converting to electronic media before doing so.

- **Can a covered entity send PHI via unencrypted e-mail? For example, a patient requests that their PHI be sent to their Yahoo or Gmail e-mail account. Is this permitted?**

The following is HHS' clarification on this topic: "We [HHS] clarify that covered entities are permitted to send individuals unencrypted e-mails if they have advised the individual of the risk, and the individual still prefers the unencrypted e-mail. We do not expect covered entities to

educate individuals about encryption technology and information security. Rather, we merely expect the covered entity to notify the individual that there may be some level of risk that the information in the e-mail could be read by a third party. If individuals are notified of the risks and still prefer unencrypted e-mail, the individual has the right to receive protected health information in that manner, and covered entities are not responsible for unauthorized access of protected health information while in transmission to the individual based on the individual's request. Further, covered entities are not responsible for safeguarding information once delivered to the individual."

- **How do the new regulations impact Health Information Exchanges, where an external (3rd party) requests access to an individual's record for treatment purposes? Because it is for treatment, payment, or healthcare operations (TPO), is an authorization not required? Or would an opt-in to the HIE be required in order for such releases to occur? Or, is no authorization or consent required to exchange information through an HIE?**

  Assuming that the requesting third party is a healthcare provider or acting on behalf of a healthcare provider, no authorization is required and no opportunity to opt out is required under HIPAA (although some states may provide a right to opt-in or opt-out of an HIE). As with current disclosures for treatment, the disclosure for HIEs does not be documented, although it may be a good idea to document the purpose of the request (i.e., an audit log indicating that the request was for treatment, or an HIE participation agreement limiting permissible requests to treatment).

- **How do you validate the signature on an authorization form with e-mail requests?**

  This is an operational process that entities must set up. Many covered entities obtain a consent form from the patient that the patient signs and indicating their e-mail address. At that point, a process may be set up to receive information from the patient via e-mail.

Request for Restrictions:

- **What if there is a balance for services not paid for? Can it be service specific? How long does the balance need to go forward without payment? If the patient pays out of pocket, how long would we hold the release to the payer? 30 days for the patient to pay? More? Less?**

  HHS provided the following on this topic: "We do not prescribe the efforts a health care provider must make but leave that up to the provider's policies and individual circumstances. While we require the provider to make a reasonable effort to secure payment from the individual, this requirement is not intended to place an additional burden on the provider but is instead intended to align with its current policies for contacting individuals to obtain an alternative form of payment to one that was dishonored. We do not require that the individual's debt be placed in collection before a provider is permitted to bill a health plan for the health care services. Further, a provider may choose to require payment in full at the time of the request for a restriction to avoid payment issues altogether. Similarly, where pre-certification is required for a health plan to pay for services, a provider may require the individual to settle payments for the care prior to providing the service and implementing a restriction to avoid the situation where the provider is unable to be reimbursed by either the individual or the health plan.

We also recognize that a provider may not be able to implement a restriction where an individual waits until care has been initiated to make such a request, such as in the case of a hospital stay, in which case the individual's protected health information may have already been disclosed to the health plan."

- **If a patient elects to pay out of pocket, even if it's Medicare, does the claim get filed?**
  HHS provided the following: "With respect to Medicare, it is our understanding that when a physician or supplier furnishes a service that is covered by Medicare, then it is subject to the mandatory claim submission provisions of section 1848(g)(4) of the Social Security Act (the Act), which requires when charges or attempts to charge a beneficiary any remuneration for a service that is covered by Medicare, then a claim must be submitted to Medicare. However, there is an exception to this rule where a beneficiary refuses to authorize the submission of a bill to Medicare. Then a Medicare provider is not required to submit a claim to Medicare for the covered service and may accept an out of pocket payment for the service from the beneficiary. The limits on what the provider may collect from the beneficiary continue to apply to charges for the covered service, notwithstanding the absence of a claim to Medicare."

- **What happens if an out of pocket service is accidently forwarded to a health plan? Does this apply only to health plans and not providers?**

  If the information is released after a restriction has been requested and paid for in advance, the provider may be subject to criminal penalties, civil money penalties, or corrective action for making an impermissible disclosure under the Privacy Rule. The government has not shown a history of attempting to penalize mistakes if reasonable systems were in place.

- **Related to the option to pay out of pocket for healthcare services to prohibit claims going to a health plan, would the patient be able to use their Health Saving Account card to pay for the medical service?**

  Yes.

- **If a patient has requested a restriction of PHI to the payer and has paid out of pocket for the service, how should subsequent service for the original service be handled?**

  If the patient returns for follow-up care and the information from the original restriction is used, the patient would once again have to pay out of pocket for the current service to ensure the information is not sent to a health payer. The provider would only send the information if requested by the payer, the information meets the minimum necessary policy of the provider, and restriction is not requested and the services paid for in advance.

- **What if the patient, based on the service that has been paid out of pocket and requested to be restricted from the payer, needs a prescription filled, how should the restriction be handled? Who's responsible for notifying the pharmacy/pharmacist to not bill the payer?**

  The patient can receive a paper prescription rather than an electronic one and take it to the pharmacy to be filled. The patient should notify the pharmacy/pharmacist of any requested restriction and pay for the prescription out of pocket.

Notice of Privacy Practices (NPP):

- **What exactly is the rule for re-distributing the NPP after significant changes have been made to it? Would the Omnibus rule changes be considered significant?**

  Yes, the rule features significant changes that require patient notification. For healthcare providers with direct treatment relationships, this means that, by the September 23, 2013 compliance date, they should have revised the notice that is posted in waiting areas, on their website, that is provided to new patients, and that is available upon request to existing patients.

- **Does the NPP have to include a statement if the covered entity plans on sending out appointment reminders?**

  Previously covered entities were required to include such a statement (per 45 CFR 164.520(b)(iii)(A)), but the new rule removes this requirement. Covered entities are free to leave this in or remove it from the notices.

- **Once changes are made to the NPP, do patients need to resign?**

  No. For healthcare providers, the final rule does not modify the current requirements to distribute revisions to the NPP. As such if a healthcare provider with a direct treatment relationship with an individual revises the NPP, the healthcare provider must make the NPP available upon request on or after the effective date of the revision and must have the NPP available at the care delivery site. They must also post the notice in a clear and prominent location. OCR clarifies that providers are not required to print and hand out a revised NPP to all individuals seeking treatment. Instead providers must post the revised NPP in a clear and prominent location and have copies of the NPP at the care delivery site for individuals to request and take with them. Providers are only required to give a copy of the NPP to, and obtain a good faith acknowledgment receipt from, new patients.

  For health plans, the rule currently requires posting the NPP on the plan's website to prominently post the material change or by the effective date of the changed notice (i.e., the compliance date of the final rule). The plan must also provide the revised notice, or information about the material change and how to obtain the revised notice, in its next annual mailing to individuals currently covered by the plan, such as at the beginning of the plan year or during the open enrollment period. Health plans that do not have customer service websites are required to provide the revised NPP, or information about the material change and how to obtain the revised notice, to individuals covered by the plan within 60 days of the notice's revision. These requirements apply to all material changes including, where applicable, the rule change adopted pursuant to GINA that prohibits most health plans from using or disclosing genetic information for underwriting purposes.

- **Has a new NPP been published?**

  Refer to the HHS/OCR collaborative Model Notices of Privacy Practice, available at http://www.healthit.gov/providers-professionals/model-notices-privacy-practices.

- **What statement(s) must be added to the new NPP?**

  Refer to AHIMA's NPP practice brief which can be found in the HIM Body of Knowledge (http://library.ahima.org/xpedio/groups/public/documents/web_assets/bok_home.hcsp), or refer to OCR's Model NPPs available online at: http://www.healthit.gov/providers-professionals/model-notices-privacy-practices.

Marketing:

- **What are some examples of marketing activity that require an authorization?**

  - Communication to former patients about a cardiac facility that is not part of the hospital that can provide a baseline EKG for $39.
  - A health insurer promoting home and casualty insurance offered by the same company.

Genetic Information Nondiscrimination Act (GINA)

- **Is it a regulation violation if a health insurance company offering an employer-sponsored group health plan uses an individual's family medical history or genetic test results, maintained in the group health plan's claims experience information, to adjust the plan's blended, aggregate premium rate for the upcoming year?**

  Yes. The issuer would be using protected health information—genetic information—for underwriting purposes, which is a violation of federal regulation 45 CFR 164.502(1)(5)(i).

- **A group health plan uses family medical history information provided by an individual, incidental to the collection of other information on a health risk assessment, to grant a premium reduction to the individual. Is this a violation?**

  Yes, the group health plan would be using genetic information for underwriting purposes, which is a violation of federal regulation *164.502 (1)(5)(i).*

- **A healthcare provider uses or discloses genetic information as it sees fit for treatment of an individual. Is this a violation?**

  No, the prohibition is limited to health plans. A healthcare provider may use or disclose genetic information.

- **A Health Maintenance Organization (HMO) acts as both a health plan and healthcare provider. Is it a violation if they use genetic information?**

  Yes and No:

  - No, if used for purposes of treatment, to determine the medical appropriateness of a benefit, and as otherwise permitted by the Privacy Rule.
  - Yes, if using the genetic information for underwriting purposes.