



HHS Issues Final Rules that Significantly Expand HIPAA Privacy & Security Regulations

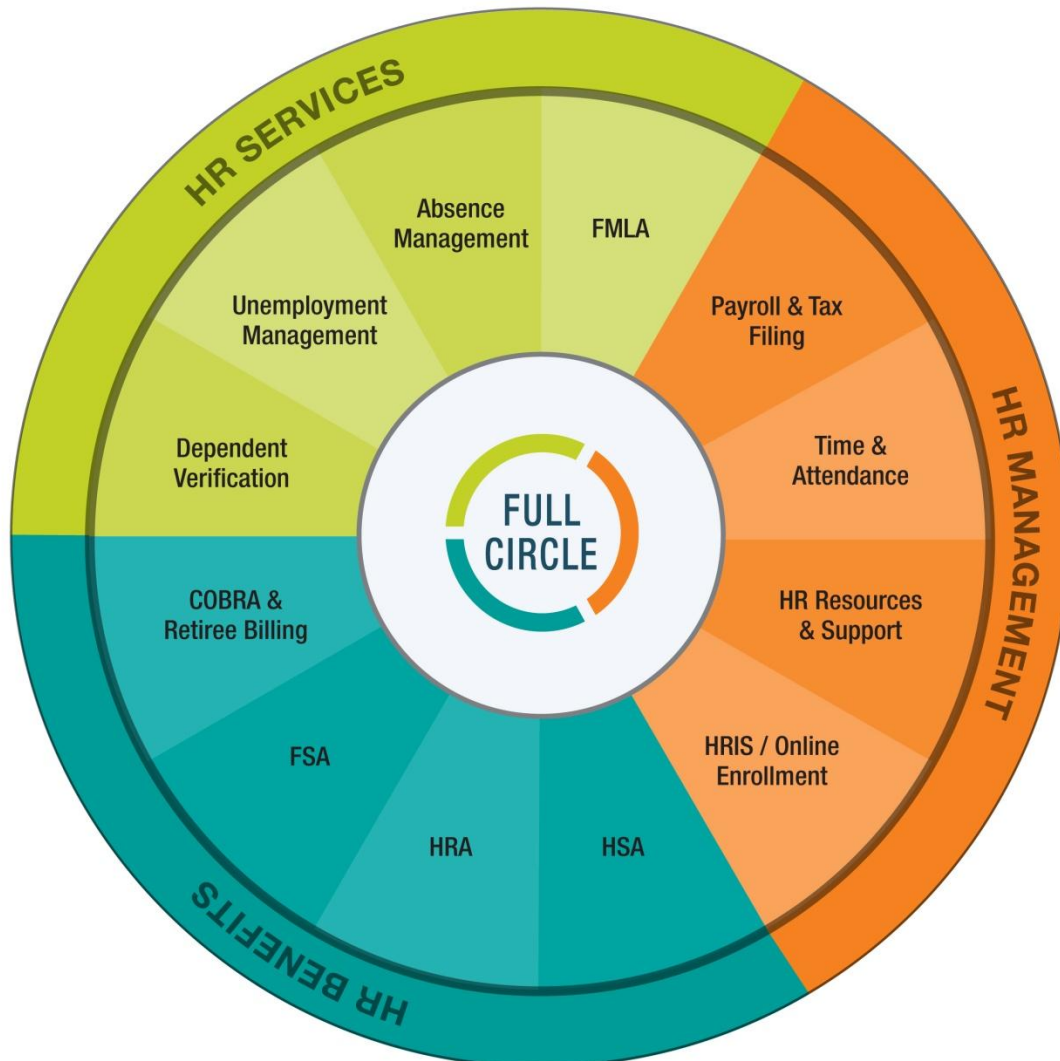
Presented by: Larry Grudzien
Attorney at Law



- HR Benefits
- HR Management
- HR Services

We're proud to offer a full-circle solution to your HR needs. BASIC offers collaboration, flexibility, stability, security, quality service and an experienced staff to meet your integrated HR, FMLA and Payroll needs.

HR Solutions Come Full Circle



HR solutions should be simple.
Keep it BASIC.

BASIC's integrated HR solutions come full circle for employers nationwide. Consistently recognized as an Inc. 5,000 Fastest Growing Private Company, our expertise allows you to control costs, manage risks and improve staff focus and effectiveness.

Topics to be Covered



- Business Associates
- Right to access PHI
- Right to restrict disclosures of PHI Security
- Breach Notifications
- Using PHI for Marketing purposes/Sale of PHI
- Disclosure of deceased individual's info to family members
- Genetic info/GINA interaction
- Updates to HIPAA Privacy Notice
- Increased enforcement
- Other provisions: Student immunization info, Hybrid-Entity rules, fundraising communications

Introduction



- On January 17, 2013, the Department of Health and Human Services (HHS) issued significant modifications to the HIPAA privacy, security, and enforcement regulations.
- The new rules, which are in final form, are applicable as of September 23, 2013, although there are some transition rules that allow for longer compliance times.

Introduction



- The new final rules will impact who is a business associate (BA) and business associate agreements (BAA), HIPAA privacy notices, the security breach notification rules, marketing communications, and an individual's right to access or restrict protected health info (PHI).
- The new final rules also expand enforcement, including making covered entities liable for acts of a BA where an “agency” relationship exists and making BAs directly liable for a number of privacy and security requirements, rather than just having contractual liability under a BAA.
- In addition, the new final rules treat certain violations under the Genetic info Nondiscrimination Act (GINA) as HIPAA privacy violations as well, which means greatly increased potential penalties under GINA.



Business Associates (BA)

BA Agreements May Need to be Updated



- In large part, the content of BAAs is the same under the final rules.
- However, the final rules include the following changes that must be incorporated into a BAA:
 - The BA must agree to comply, where applicable, with the HIPAA security standards with respect to electronic PHI. *Note: Before, this was not an express requirement, although most BAAs likely required compliance with all of HIPAA, so may not be a substantive difference.*
 - The BA must agree to report any breaches of unsecured PHI as required under the security breach rules. *Note: This requirement has been applicable since the interim final rule on security breach notifications, but not an express requirement of the BAA.*

BA Agreements May Need to be Updated (Continued)



- The BA must require subcontractors that create, receive, maintain, or transmit PHI on behalf of the BA to agree to the same restrictions and conditions as the BA. *Note: This language has been slightly re-worded from the prior rule.*
- The BA must agree that, to the extent the BA is to carry out a covered entity's obligations under the privacy rule that it will comply with the requirements of the privacy rule that apply to the covered entity. *Note: Again, this likely was included – or at least intended – in prior BAAs, but now is an express requirement.*
- HHS has provided a sample BAA based on the new final rules at <http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html>

Transition Period for Updating BAAs



- While the general applicability date for the new rules is 9/23/14, the final rule provides a transition period for updating BAAs where there is already a BAA in place.
- These BAAs must be updated by the earlier of:
 - the next renewal after 9/23/13 or 9/23/14.
- The Preamble clarifies that the HIPAA requirements apply in substance – the transition rule only applies to the documentation of these rules in the BAA.

Transition Period for Updating BAAs



- This special transition rule only applies where there was a BAA in place as of 1/25/13 - the date the final rules were issued - and the underlying contract between the plan and BA is not renewed between 3/26/13 - the “effective date” of the rules and 9/23/13 - the “applicability date” of the rules.
- Plans and BAs that do renew their contracts between 3/26/13 and 9/23/13 must have a compliant BAA as of 9/23/13.
- Any new BAAs entered into on or after 9/23/13 must meet the new requirements, but as a practical matter, plans and BAs may want to well.

Subcontractors Also Need BAAs



- The new rules require that BAs not only have a BAA in place with the covered entity to whom they are providing services, but also with any subcontractors that use PHI of the covered entity.
- This is a new requirement that will significantly impact BAs and their subcontractors.
- The Preamble to the rules clarifies that subcontractors also will need BAAs with their subcontractors "no matter how far down the chain" as long as PHI is being used.
- In addition, the subcontractor BAA must be at least as stringent as the BAA above it.
- BAs and subcontractors can use the same transition rules that apply to covered entities and base the applicability date of the subcontractor BAA on the covered entity's contract renewal date with the BA.

Data Transmission & Network Services



- The new rules state that a BA includes a Health Info Organization, E-prescribing Gateway, or other person that provides data transmission services to a covered entity that requires access to PHI on a “routine basis.”
- The Preamble clarified that entities that manage the exchange of PHI through a network, including those providing record locator services or performing oversight and governance functions for an electronic health info exchange have more than "random access" and would be considered BAs.

Personal Health Record (PHR) Vendors



- The new rules also define a BA to include a party offering PHRs on behalf of a covered entity.
- The Preamble clarifies that the rules do not apply to PHR vendors who are considered to act for the individual and who have an individual's authorization to access a covered entity's data, even if the PHR vendor has an agreement with the covered entity regarding the exchange of data, such as technical specifications.

Mere Conduit Exception



- Where a third party does not require access to PHI on a “routine basis,” it may be acting as a "mere conduit" for the transport of PHI and not be considered a BA.
- The Preamble says that the "conduit" exception is narrow and intended to exclude only those entities providing mere courier service like the US Postal Service or UPS and their electronic equivalents, such as Internet service providers (ISPs) providing mere data transmission services.
- HHS says that whether the conduit exception applies is fact specific based on the nature of service provided.
- For example, a telecommunications company that has occasional random access to PHI to review whether data transmitted over its network arrives at its intended destination may be a conduit and, in that case, would not be considered a BA.

BA Liability



- Under HITECH and the new rules, BAs (as well as subcontractors) are directly liable and can be penalized by HHS for:
 - Impermissible uses and disclosures of PHI
 - Failure to provide breach notification to the covered entity
 - Failure to provide access to a copy of electronic PHI to the covered entity, the individual, or the individual's designees (whichever is specified in the BAA)
 - Failure to disclose PHI where required by HHS to investigate or determine the BA's compliance with HIPAA
 - Failure to provide an accounting of disclosures (under the proposed accounting rule, which has not yet been finalized)
 - Failure to comply with the HIPAA Security Standards (including appointing a security official and completing a security risk assessment)
- BAs remain contractually liable for other requirements of the BAA.
- The Preamble clarifies that BAs are not required to provide a privacy notice or designate a privacy official unless otherwise agree to in the BAA

Covered Entity May be Liable for BA's Actions



- The new rules make the covered entity liable for the acts of BAs who are “agents” (and the BA liable for acts of subcontractors who are “agents”) under the federal common law of agency, where the BA or subcontractor is acting within their scope as agent.
- The Preamble says that an analysis of whether a BA is an agent will be fact specific, taking into account the terms of the BAA as well as the totality of the circumstances.
- HHS notes that labels given to the parties do not necessarily control whether an agency relationship exists.
- Rather, the Preamble says that the essential factor in determining whether an agency relationship exists is the “right or authority of the covered entity to control the BA’s conduct in the course of performing a service on behalf of the covered entity.”
- The Preamble provides an example where the BAA says that a BA must mail PHI available based on the instructions to be provided or under direction of the covered entity and says that this type of provision would create an agency relationship because the covered entity has a right to give interim instruction and direction during the course of the relationship.



Right to Access PHI

Disclosure in Electronic Form



- Under the new rules, if the info is maintained electronically, the individual has a right to request the info in electronic form.
- The plan must provide the info in the form and format requested by the individual within 30 days (plus a 30-day extension) if the info is "readily producible" - for example, in Word, Excel, text, or HTML.
- If not readily producible, the plan must provide in a readable electronic form as agreed to by the parties.

Disclosure in Electronic Form



- In any event, a plan cannot deny providing the info electronically, and the Preamble to the rules suggests that the plan at least be able to provide the info in PDF form.
- The Preamble also notes that if the info includes electronic links or attachments, this info also must be included in the electronic copy.
- The plan is permitted to charge for labor and supplies, such as where an individual requests that electronic info be provided on portable media like a flash drive.

Request to Forward to Third Party



- The rules also state that an individual is permitted to designate a third party to receive the info, and the plan must comply.
- The rule requires that the designation must be in writing, clearly designate the third party, and be signed by the individual.
- The Preamble clarifies that an individual can request that the info be emailed to him or her, even in non-encrypted form.



Right to Restrict Disclosures of PHI

Must Restrict Disclosure Where Individual Paid the Cost Themselves



- The new rule requires the covered entity to agree to the restriction where the disclosure would be to a health plan for payment or health care operations purposes and the individual has paid out of pocket in full for the service.
- The Preamble notes that covered entities will need to use some method to flag PHI that has been restricted.
- However, providers are not required to notify "downstream providers" of the restriction.
- Rather, it is the individual's obligation to request restrictions from subsequent providers.

Bundled Services



- Regarding services that are "bundled" and for which an individual only has paid out of pocket for some services, the provider must restrict disclosure of the services for which the individual has paid out of pocket if possible.
- If not, the provider should counsel the individual about which services will be disclosed and give the individual an opportunity to pay out of pocket for all services in the bundle.

Application to Health Plans?



- The rule applies to covered entities disclosing PHI to a health plan, which most likely will include disclosures by providers to health plans, but technically could include disclosures from one health plan to another health plan.
- The Preamble notes that the rule, "in effect, will apply only to covered health care providers," and all examples HHS provides relate to providers.
- The Preamble also says that only providers are required to include this additional right to restrict info in their Notice of Privacy Practices.

Application to Health Plans?



- More likely, health plans will be indirectly impacted by possibly having gaps in their claims info.
- The Preamble does clarify that if an individual pays out of pocket and requests a restriction for a service, but does not pay out of pocket for follow-up care, the provider may need to include info about the initial care that was previously restricted in order to have the service deemed medically necessary.
- The Preamble encourages the provider to have an "open dialogue" with the individual to ensure they are aware that prior info may need to be disclosed unless the individual pays out of pocket for the follow-up service.

Application to HMOs



- If a provider within an HMO is restricted by law from accepting out of pocket payments from individuals, the Preamble says that the provider may counsel the individual that he or she may need to use an out-of-network provider in order to restrict disclosure.
- However, the Preamble notes that a contractual requirement that the HMO provider submit all claims to the HMO would not be considered "required by law," and in that case, the provider must comply.
- The Preamble says that HMO providers may need to update their contracts with the HMO in the interim time until the requirement applies - 9/23/13.

Application to FSAs & HSAs



- If an individual pays for services with funds from a Flexible Spending Account (FSA) or Health Savings Account (HSA), the individual still will be considered to have paid out of pocket, so still has a right to request a restriction on disclosures of PHI related to the service.
- However, the individual may not strict disclosures to the FSA or HSA where necessary to effectuate payment.
- This new provision would not apply to health reimbursement arrangements (HRAs) because HRAs are funded by the employer.



Security Breach Notifications

Burden on Plan/Harm Threshold Replaced with “Compromised” Standard



- Under the new rules, a “breach” is an acquisition, access, use, or disclosure of PHI in a manner not permitted by the HIPAA privacy and security rules that “compromises” the security or privacy of the PHI.
- HHS said that some had interpreted the “harm threshold” in the interim final rule as setting a higher threshold for breach notification than HHS had intended.
- HHS said that this change was to clarify its position that a breach notification is necessary in all situations except those in which the covered entity or BA demonstrates that there is a “low probability” that the PHI has been “compromised.”

Burden on Plan/Harm Threshold Replaced with “Compromised” Standard



- The Preamble states that the burden is on the covered entity or BA to demonstrate that either an impermissible use did not constitute a breach or that the proper notifications were made.
- The Preamble says that the plan must conduct a risk assessment to make this determination and must maintain documentation sufficient to meet the burden of proof.
- The Preamble states that a violation of the “minimum necessary” rule under HIPAA could be considered a breach.

Failure to Consider



- The new rules provide that the plan's risk assessment must include at least the following factors:
 - the nature and extent of the PHI involved
 - the unauthorized person who used the PHI or to whom the disclosure was made
 - whether the PHI was actually acquired or viewed
 - the extent to which risk has been mitigated

Failure to Consider



- The Preamble provides an example where a covered entity misdirects a fax containing PHI to the wrong physician practice.
- Upon receipt, the physician calls the covered entity to say he has received the fax in error and destroyed it.
- The Preamble says that, after a risk assessment considering the above factors, a covered entity may determine there was a low probability of the info being compromised, so there would be no breach notification requirement.

Exceptions



- Generally, the exceptions to the rule remain the same.
- However, the new rules remove the exception for limited data sets that do not contain dates of birth or zip codes.
- Under the new rule, if there is an impermissible disclosure from such a limited data set, the plan must conduct a risk assessment under the normal rules.
- The safe harbor for (when performed under the adopted technical notices) remains.

Specific Notification Requirements



- The content required to be included in a notification is the same as in the interim final rule, along with the timeframes and parameters for providing notifications to individuals, HHS, and the media.
- The Preamble did clarify that one notification could be sent to a participant and spouse or other dependents residing at the same address and that an electronic notice could be provided where the individual “affirmatively” agrees.

BAs



- The new rules require that the BAA address the security breach rules and adopt the prior requirement that the BA notify the covered entity within 60 days of discovery of the breach and then the covered entity has 60 days to make the required notifications.
- The final rule also adopts the exception where the BA is acting as an “agent” for the covered entity, in which case the two are treated as one entity, and the covered entity must make the required notifications within 60 days of the BA’s discovery.
- The Preamble says that whether a BA is considered an “agent” will be based on facts and circumstances, taking into account federal common law and the covered entity’s ability to control the BA’s actions.
- The Preamble also notes that if the covered entity and the BA disagree as to whether a disclosure is a “breach,” the burden is ultimately on the covered entity to show that there was low probability of the info being compromised.



Using PHI for Marketing Purposed/Sales of PHI

If Remuneration Involved, Will Be Marketing



- The new rules largely retain the exceptions to the marketing definition listed above, but add that if the health plan receives "financial remuneration" in exchange for the communication, the communication will be considered marketing and only may be made if authorized by the individual.
- The authorization must expressly state that remuneration is involved, but the Preamble notes that the authorization is not required to be limited to a single product or service.
- Rather, the authorization may be more open-ended to "apply to subsidized communications generally."

What is Financial Remuneration?



- The rules define "financial remuneration" as direct or indirect payment from or on behalf of a third party whose product or service is being described.
- The Preamble clarifies that financial remuneration only includes financial payments made in exchange for making the communication and not "in kind" benefits.
- In addition, in order to trigger the authorization requirement, the purpose of the communication must be to promote the third party's product or services.
- If a third party provides financial remuneration to a health plan to implement a disease management program, the plan could send communications about the disease management program without authorization because the plan would be promoting its own program, rather than the third party's program.

Exception for Face-to-Face Communications/Nominal Gifts



- The final rule retains the exceptions for face-to-face communications, but HHS notes that email or phone communications would fall under the general rule in the previous slide.
- The final rule also retains the exception related to gifts of nominal value.

Exception for Communication About Current Drugs



- In addition, the final rules add an exception allowing refill reminders or other communications about a drug or biologic currently prescribed for an individual, even if the covered entity receives financial remuneration from the third party (e.g., pharmaceutical company).
- The Preamble provides that this exception would include communications about generic equivalents of drugs an individual is prescribed, adherence communications, and communications about all aspects of the drug delivery system, such as info about insulin pumps.
- The remuneration must be reasonably related to the cost of taking the communication, which HHS says includes only the cost of labor, supplies, and postage to make the communication.

Exception for Communications About Current Drugs



- The Preamble provides an example where a drug manufacturer provides financial remuneration to a pharmacy to provide refill reminders.
- The example says that this type of communication would be permitted without authorization as long as the remuneration only covers the cost to draft, print, and mail the communication.
- However, if the drug manufacturer provides an additional financial incentive, the pharmacy must obtain authorization - unless the communication is given to the individual as part of a face-to-face communication (under the exception described above)

Other Exceptions



- The Preamble also clarifies that the marketing restriction does not apply to communications to promote health in general that does not promote a product or service, such as annual mammogram reminders.
- In addition, HHS says that the restrictions do not apply to communications about government-sponsored programs, such as Medicare or Medicaid, because there is no "commercial component."

Sale of PHI



- The new rules also require authorization if the plan sells PHI.
- The authorization must state that the disclosure involves remuneration.
- The regulations define "sale" of PHI to include where the plan directly or indirectly receives remuneration from the recipient of the PHI.

Sale of PHI



- The Preamble makes clear that, unlike marketing, remuneration here includes financial or nonfinancial (i.e., in-kind) benefits and provides an example where a third party offers a covered entity computers in exchange for disclosing PHI (even for a permitted reason) but then allows the covered entity to use the computers for other reasons or to retain after the allowed disclosures have been made.
- The Preamble clarifies that the limitation on sale of PHI does not apply to exchange of remuneration to BAs performing a plan function or to disclosures within single legal entity or among affiliated covered entities - only outside the entity.



Disclosure of Deceased Individual's Info to Family Members

Disclosure to Family Members & Others Involved in Care



- The new rule extend this provision to deceased individuals and allows a plan to disclose a decedent's PHI to a family member or others who were involved in the care or payment for care prior to death, unless doing so is "inconsistent with any prior expressed preference of the individual that is known" to the plan.
- The Preamble expressly states that this group could include spouse, parents, children, domestic partners, other relatives, or friends of a decedent.
- The Preamble clarifies that the info provided must be limited to info that is relevant to the person's involvement and provides an example where a provider may disclose billing info to a family member assisting with the estate, but could not share info about past, unrelated medical problems.

Disclosure to Family Members & Others Involved in Care



- The Preamble says that, in some cases, it will be readily apparent that a family member or other person has been involved in the individual's care, such as someone having been identified by the decedent or someone who has made prior inquiries.
- In other cases, the covered entity needs to “just have reasonable assurance” that the person is a family member or other person involved in the individual’s care or payment for care.
- The Preamble says, for example, the person may indicate how they are related to the decedent or other sufficient details about the decedent’s circumstances to indicate involvement.

No Longer PHI After 50 Years



- The new rules also provide that info no longer will be considered PHI once the individual has been deceased for 50 years.



Genetic Info/Overlap with GINA

Genetic Info is PHI



- The new rules clarify that genetic info is PHI (this is not really new - plans likely considered this info to be PHI all along).

Genetic Violations are now HIPAA Violations



- The new rules prohibit a health plan from “underwriting” based on genetic info and adopt the definition of “underwriting” from Title I of GINA and its implementing regulations.
- This means that a violation of the GINA underwriting rules will now be a HIPAA privacy violation.
- The Preamble provides two examples of prohibited types of underwriting: where an insurer uses family medical history or results from genetic tests to adjust the plan’s aggregate premium or where a group health plan grants a premium reduction to an individual based on collection of family medical history on a health risk assessment.

Expansion of Entities Subject to GINA to Include HIPAA Excepted Benefits (Except Long-Term Care)



- Currently, GINA applies to group health plans under the HIPAA portability rule, but does not apply to HIPAA excepted benefits, such as limited scope dental and vision, supplemental plans, disease only plans, fixed indemnity coverage, and long-term care coverage.
- The HIPAA privacy rules (even the current rules) do not adopt all of HIPAA's excepted benefits, so the above listed plans that may be excepted from the HIPAA portability rules are subject to the HIPAA privacy rules.
- The new final privacy rules, which prohibit underwriting based on genetic info, extend this prohibition to all covered entity health plans, except long-term care.

Expansion of Entities Subject to GINA to Include HIPAA Excepted Benefits (Except Long-Term Care)



- This means that HIPAA excepted benefits that do not currently have to comply with GINA will be subject not only to the confidentiality provisions of the HIPAA privacy rules but also several of the prohibitions found in the GINA statute.
- The Preamble says that HHS did not extend this liability to long-term care coverage because it simply did not have enough info about whether prohibiting underwriting based on genetic info would impact this industry, but it will reassess as it receives more info.
- The Preamble also clarifies that the extension of GINA's underwriting rules does not apply to covered entity health care providers.

Notice of Privacy Practices



- The new rules require health plans that perform underwriting to include a statement in their HIPAA Privacy Notices that they are prohibited from using or disclosing genetic info for such purposes (except for long-term care issuers).



Updates to HIPAA Privacy Notice

Updated Content



- The new rules require that the privacy notice be updated to include the following:
 - A description of the type of uses and disclosures that require an authorization, including when related to psychotherapy notes (where applicable for that covered entity), for marketing purposes, or related to the sale of PHI
 - A statement that other uses and disclosures not described in the notice will be made only with the individual's written authorization, which the individual may revoke
 - Where a covered entity intends to engage in fundraising activities, that the individual has a right to opt out of receiving such communications
 - Where a covered entity (except a long-term care issuer) intends to use or disclose PHI for underwriting purposes, a statement that the covered entity is prohibited from using or disclosing genetic info for such purposes
 - Statement that a covered entity is not required to agree to a requested restriction on disclosures of PHI to a health plan where the individual has paid out of pocket in full for the service (the Preamble notes that this requirement only applies to health care providers)
 - A statement that the covered entity will notify affected individuals following a breach of unsecured PHI.

Due Dates for Delivery



- The Preamble provides two rules regarding delivery of the new, updated notice, depending on whether the plan posts its notice on its website:
 - If the plan posts its current privacy notice on its website, it must update that online notice by 9/23/13 and then deliver notices to individuals as part of its next annual mailing.
 - If the plan does not post its current privacy notice on its website, it must deliver notices to individuals within 60 days of the required 9/23/13 applicability date (or 11/23/13).



Increased Enforcement

Penalties



- The HITECH Act significantly increased the penalty amounts for HIPAA violations, and these penalties were re-stated in the regulation.
- HHS generally is required to issue a penalty unless the covered entity or BA can show that the violation is not due to willful neglect and is corrected within 30 days, beginning on the first date the covered entity or BA knew, or by exercising reasonable diligence, would have known that the violation occurred.
- Factors to determine the penalty amount include the nature and extent of the violation; the physical, financial, or reputational harm resulting from the violation; history of prior compliance (or violations) by the covered entity or BA; and the financial condition of the covered entity or BA that may impact its ability to comply.
- The final rule also expressly allows HHS to coordinate with other law enforcement agencies, such as State Attorneys General or the FTC in pursuing remedies available to these parties.

Willful Neglect



- Where a violation may involve “willful neglect,” the new rules remove some of HHS’s discretion and require HHS to investigate.
- The regulations define “willful neglect” to mean conscious, intentional failure or reckless indifference to the obligation to comply.
- The new rules provide that HHS “will” investigate a complaint when a preliminary review of the facts indicates a “possible” violation due to willful neglect.
- HHS “may” investigate other complaints.
- HHS still has authority to attempt to reach a resolution through “informal means,” which may include a covered entity demonstrating compliance or completing a corrective action plan, but HHS is not required to use informal means when the violation is due to willful neglect and may issue a penalty instead.

Summary of Penalties



- *Tier 1:* For violations in which it is established that the covered entity of BA did not know and, by exercising reasonable diligence, would not have known that the covered entity violated a provision, an amount not less than \$100 or more than \$50,000 for each violation.
- *Tier 2:* For a violation in which it is established that the violation was due to reasonable cause and not to willful neglect, an amount not less than \$1000 or more than \$50,000 for each violation.
- *Tier 3:* For a violation in which it is established that the violation was due to willful neglect and was timely corrected, an amount not less than \$10,000 or more than \$50,000 for each violation
- *Tier 4:* For a violation in which it is established that the violation was due to willful neglect and was not timely corrected, an amount not less than \$50,000 for each violation.



Other Changes

Other Individual Rights



- The new rules did not change the provisions related to an individual's right to amend PHI, request confidential communications, or request an accounting of certain PHI disclosures.
- Note that HHS issued proposed accounting rules in May 2011, which would have required covered entities, including BAs, to keep a log of anyone who accessed electronic PHI and provide an access report to individuals upon request.
- This would be a significant new requirement that even HHS recognized goes beyond the requirements of the HITECH Act.

Note: This will be an area to watch.

Student Immunization Info



- The new rules revise the exception for disclosures for public health activities to allow a covered entity to disclose immunization info to a school where state or other law requires the school to have such info prior to a student's admission, provided the info is limited to proof of immunization.
- The covered entity still will be required to document an obtain some type of agreement from the parent or guardian (or individual if an adult or emancipated minor).
- The Preamble says that this agreement must be affirmative (rather than an opt out or negative election), but the agreement may be oral.

Fundraising Communications



- The new rules allow a covered entity to use or disclose the following PHI with respect to its own fundraising purposes, such as a hospital sending targeted fundraising invitations to former patients: name and contact info, date of birth, dates of care, department of service, treating physician, outcome info, and health insurance status.
- The covered entity may use or disclose this info only if each fundraising communication provides a clear and conspicuous opportunity for the recipient to elect not to receive further fundraising communications.
- This notice also must appear in the Notice of Privacy Practices.

Hybrid Entity Rules



- A hybrid entity is an entity that includes both health care and non-health care components, such as an insurer that provides both medical and disability policies.
- The current rules allow such an entity to designate its health care components and limit HIPAA applicability to those health care components.
- However, where a covered entity has made these designations, it must have some type of “firewall” between health and non-health components and treat disclosures from a health care component to a non-health care component as a disclosure to a third party.
- In some cases, this could include BA functions that the covered entity is providing to itself, such as a company providing TPA services to its own health plan.
- The new rules require that a health care component of a hybrid entity include all BA functions within the entity.



Questions



- HR Benefits
- HR Management
- HR Services

We're proud to offer a full-circle solution to your HR needs. BASIC offers collaboration, flexibility, stability, security, quality service and an experienced staff to meet your integrated HR, FMLA and Payroll needs.



Contact Larry



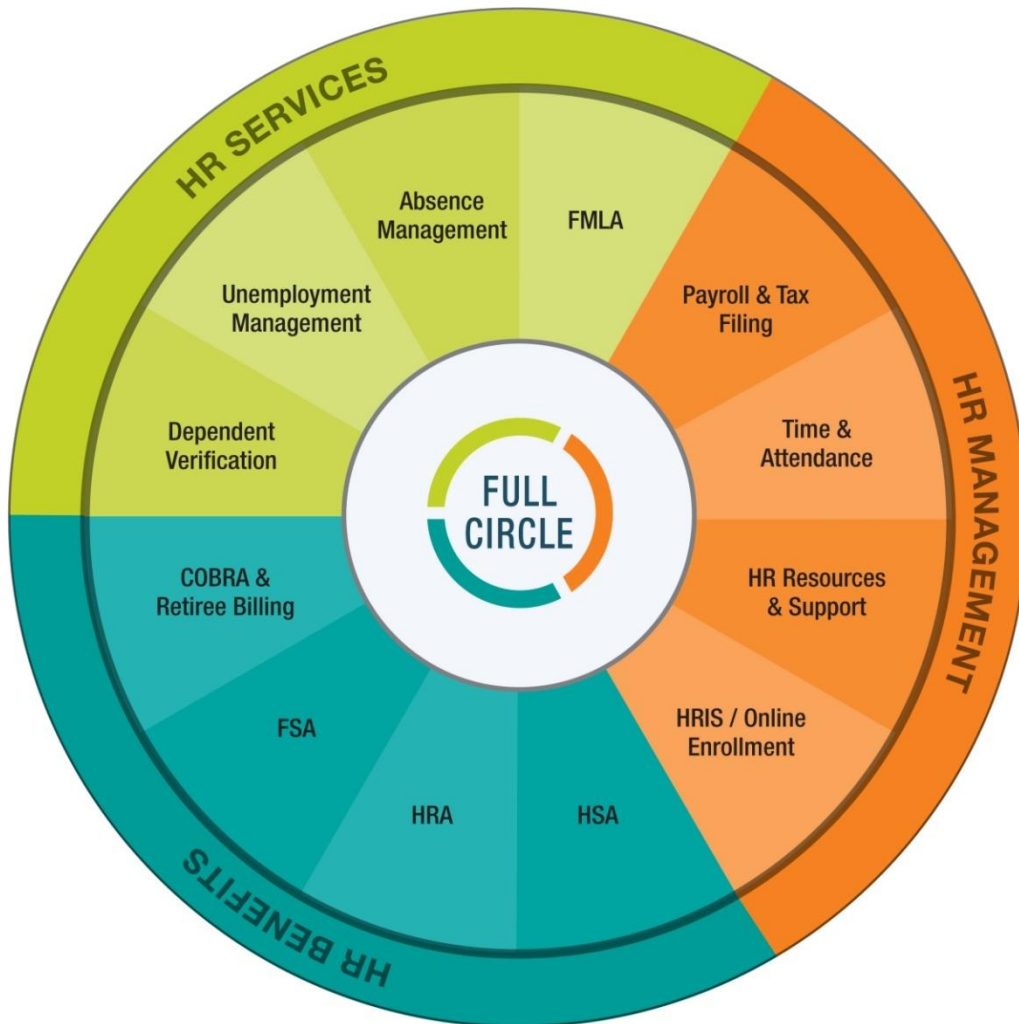
Larry Grudzien

Phone: 708.717.9638

Email: larry@larrygrudzien.com

Website: www.larrygrudzien.com

Contact Us



HR solutions should be simple.
Keep it BASIC.



800.444.1922
sales@basiconline.com