Colorado Medical Society

The HIPAA OMNIBUS RULE

June 3, 2013

Presented by
David A. Ginsberg
President, PrivaPlan Associates, Inc.®

PrivaPlan

Agenda

- The HIPAA "Omnibus Rule"-**a high level overview**
- Effective dates
- Specific provisions and changes
- Special focus on Breach notification

PrivaPlan

Why this seminar?

- January 25, 2013 the Final Rule was published
- The full title is:

"45 CFR Parts 160 and 164 Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules"

PrivaPlan

Why this seminar?

These modifications pertain to four different areas of HIPAA :

- The Privacy Rule
- The Security Rule
- The Enforcement Rule
- The Breach Notification Rule

PrivaPlan

Back to the Basics-context for today

- HIPAA covers these primary compliance areas:
  - Privacy
  - Security
  - Administrative Simplification-Transactions and Code Sets
  - With the 2009 ARRA/HITECH Acts-Breach Notification
  - Enforcement regulations for the above

PrivaPlan

ARRA and HIPAA

- The American Recovery and Reinvestment Act of 2009 ("ARRA") privacy and security provisions are part of the Health Information Technology for Economic and Clinical Health Act ("HITECH Act") within ARRA
- These pertain to the overall initiative to promote adoption and use of electronic health records and health information technology
- These recognize the vulnerabilities created by adoption of EHR and HIT and especially promotion of a personal health record and health information exchanges

PrivaPlan

HITECH Privacy and Security-Key Provisions

- Breach Notification Rule
- Business Associates-Expansion of applicability
- New Enforcement Rules
- Accounting of Disclosures
- Access and restriction rights
- Limited Data Set-Minimum Necessary
- Marketing and fundraising restrictions
- PHRs

PrivaPlan

Omnibus Rule

- The Omnibus Rule provided modifications to all of these areas except for Personal Health Records (PHR's are to some extent governed under HIPAA Privacy already, and vendors of PHR systems are governed under Federal Trade Commission law in the event of a breach of unsecured information)
- Accounting of Disclosures-a final rule will be issued later on this
- The Omnibus Rule also added or expanded on compliance areas

PrivaPlan

Specific Rulemaking already released

- Privacy Rule-April 16, 2003
- Security Rule-April 20, 2005
- Transactions and Code Set Rule-October 2003
- Breach Notification Rule-August 2009; effective September 23, 2009 with enforcement effective as of February 22, 2010 as the Interim Final Rule
- Enforcement Penalty Changes-IFR November 30, 2009
- It took from 2010 until now for the Office of Civil Rights within HHS to release the final Breach Notification Rule which is one of the four major rule changes within the recently released Omnibus Rule

PrivaPlan

Compliance timelines

- Omnibus changes are in effect as of March 2013; however in most cases there is a 180 day implementation period

- "During the 180 day period before compliance with this final rule is required (September 23, 2013), covered entities and business associates are still required to comply with the requirements of the interim final rule"—(Breach Notification)-and other existing requirements!

PrivaPlan

Changes-Special Privacy Protections

- Disclosures to health plans – At the patient's request, physicians may not disclose information about care the patient has paid for out-of-pocket to health plans, unless for treatment purposes or in the rare event the disclosure is required by law. This change updates the previous HIPAA Privacy Rule individual rights to special privacy protections.

Changes-Special Privacy Protections

Previously, physicians could refuse a request for restrictions on use and disclosure of PHI. The new law *requires* restrictions when the patient has paid out-of-pocket and requests the restriction

This change is likely to have the greatest impact on your practice workflow both in terms of documentation and follow up to ensure the restriction is adhered to

Changes-Special Privacy Protections

For example:

- How should you document the request?
- What happens if the payment made is rescinded?
- What about downstream releases…to HIE's or other providers?
- And most importantly-what functionality is needed with your practice management or EHR systems to assure the restriction is followed?

PrivaPlan

Changes-Immunization data

- Childhood immunizations – Under the new rules, physicians may disclose immunizations to schools required to obtain proof of immunization prior to admitting the student so long as the physicians have and document the patient or patient's legal representative's "informal agreement" to the disclosure.
- The release cannot be to the school at their request only-affirmative request from the parent/ guardian/patient is still necessary

PrivaPlan

Changes-Immunization data

- The change is primarily to reduce the burden of documentation for such routine releases
- There is still a need to ensure that the release is per State or other law-otherwise revert to the use of a written authorization!
- And there is a stated requirement to document the agreement to release immunization information

Changes-Access and Copies

- Decedents – The new rules allow physicians to make disclosures to the deceased's family and friends under essentially the same circumstances such disclosures were permitted when the patient was alive, that is, when these individuals were involved in providing care or payment for care and the physician is unaware of any expressed preference to the contrary. The new rule also eliminates any HIPAA protection for PHI 50 years after a patient's death .

Changes-Access and Copies

- Copies of *e*PHI – Under HIPAA Physicians will now have only 30 days to respond to a patient's written request for his or her PHI with one 30 day extension (compared to the current allowance under HIPAA of one 60 day extension), regardless of where the records are kept. They must provide access to EHR records in the electronic form and format requested by the individual if the records are "readily reproducible" in that format

PrivaPlan

Changes-Access and Copies

- Otherwise you must provide the records in another mutually agreeable electronic format. Hard copies are permitted only when the individual rejects all readily reproducible *e*formats
- Physicians must also consider transmission security, and may send PHI in unencrypted emails only if the requesting individual is advised of the risk and still requests that form of transmission.

PrivaPlan

Changes-Access and Copies

- The allowance to use email to transmit electronic copies has many associated workflow issues
- This pertains to "PHI that is the subject of the request…maintained electronically in one or more electronic designated record sets.."-NOT JUST EHR records! But it is relevant for CE's who use an EHR…
- How will you document advisement of risk?
- Requests should always be handled in writing and signed by the patient/personal representative

PrivaPlan

Changes-Access and Copies

- "We clarify that covered entities are permitted to send individuals unencrypted emails if they have advised the individual of the risk, and the individual still prefers the unencrypted email"
- "If individuals are notified of the risks and still prefer unencrypted email, the individual has the right to receive protected health information in that way, 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"

PrivaPlan

Changes-Access and Copies

- Does this open the door for emailing PHI?
- Definitely NOT-just in this situation
- Other emailing should still be done in a secured fashion
- We believe the risk is too great to assume a blanket email of PHI program-without using secured email and better yet-patient portals (since you will have a Stage 2 MU benefit)
- Remember the risk is less about interception and more about sending to the wrong party!

PrivaPlan

Changes-Access and Copies

- Be sure to update your Designated Record Set definition
- Some medical practices will have more than just EHR data in an electronic designated record set
  - Imaging?
  - Old practice management applications?
  - Web applications

PrivaPlan

Changes-Copies

- Charging for copies of ePHI or PHI-The new rule modifies the costs that can modified the section relative to the costs that may be charged to the individual for copy requests by limiting the cost to is labor costs and supply costs if the patient requests a paper copy, or if electronic the cost of any portable media (such as a USB memory stick or a CD)
- Labor can include the skilled time to create and copy the file-at a reasonable cost based rate

PrivaPlan

Changes-Copies

- Is Colorado law more stringent regarding copy fees?

PrivaPlan

Changes-Minimum necessary

- Minimum necessary is reiterated to include or apply to business associates
- However, we encourage all participants to review their Minimum necessary procedures and practices and ensure these are in place
- We also encourage all participants to update their designated record set definitions, especially in light of current or anticipated use of EHRs

PrivaPlan

Changes-Sale of PHI

- Sale of PHI – The new rules clarify that the prohibition on the sale of PHI in the absence of the patient's written authorization extends to licenses or lease agreements, and to the receipt of financial or in-kind benefits
- It also includes disclosures in conjunction with research if the remuneration received includes any profit margin

PrivaPlan

Changes-Sale of PHI

- Prohibition on PHI sales does not extend to permitted disclosures for payment or treatment nor to permitted disclosures to patients or their designees in exchange for a reasonable cost-based fee

Changes-Marketing

- Marketing communications – The new rules further limit the circumstances when physicians may provide marketing communications to their patients in the absence of the patient's written authorization. Generally speaking, the only time a physician may tell a patient about a third-party's product or service without the patient's authorization is when

1) the physician receives no compensation for the communication

Changes-Marketing

- 2) the communication involves a drug or biologic the patient is currently being prescribed and the payment is limited to reasonable reimbursement of the costs of the communication (no profit); 3) the communication involves general health promotion, like routine diagnostic tests; or 4) the communication involves government or government-sponsored programs

PrivaPlan

Changes-Fundraising

- This is applicable to those physicians in organizations that conduct fundraising such as not for profit hospitals, Community Health Clinics and so forth
- New requirements for language in the Notice of Privacy Practices to disclose that fundraising activities take place and PHI may be used for these purposes

PrivaPlan

Changes-Fundraising

- With each fundraising communication to a patient physicians must give clear and conspicuous information about how to opt out of future fundraising communications
- If an opt out is exercised it must be followed going forward
- Treatment may not be conditioned on the authorization to receive fundraising communications

PrivaPlan

Changes-Authorizations

- Research authorizations – The new rules permit physicians to combine conditioned and unconditioned authorizations for research participation, provided individuals can opt-in to the unconditioned research activity. Moreover, these authorizations may encompass future research.

PrivaPlan

Changes-Notice of Privacy Practices

- Physicians must amend their NPPs to reflect the changes set forth above including those related to breach notification, disclosures to health plans, and marketing and sale of PHI
- As the rules presume these are all material changes, physicians will have to post the revised NPP, and make copies available at their office, to all new patients and to any one else on request.

PrivaPlan

Changes-Notice of Privacy Practices

- Physicians who maintain a website, are cautioned to post the updated NPP on their website as required by the existing HIPAA Privacy rule
- The new rules also eliminate requirements to include information on communications concerning appointment reminders, treatment alternatives or health-related benefits or services in NPPs, but the rules do not require that that information be removed either

PrivaPlan

Changes-Notice of Privacy Practices

- Physicians who maintain a website, are cautioned to post the updated NPP on their website as required by the existing HIPAA Privacy rule
- The new rules also eliminate requirements to include information on communications concerning appointment reminders, treatment alternatives or health-related benefits or services in NPPs, but the rules do not require that that information be removed either

PrivaPlan

Changes-Notice of Privacy Practices

- Look for a new PrivaPlan NPP template in both English and Spanish
- Most of the changes are already incorporated in the most recent (2010) PrivaPlan NPP template

PrivaPlan

Changes-Business Associates

- The new rules expand the universe of individuals and companies which must be treated as business associates to include Patient Safety Organizations and others involved in patient safety activities, health information organizations like *e*prescribing gateways or health information exchanges that transmit and maintain PHI and personal health record vendors physicians sponsor for their patients

PrivaPlan

Changes-Business Associates

- Thus, physicians must review their relationships and determine if they must enter new BA agreements with these entities or others that create, receive, store, maintain or transmit PHI on their behalf
- A new definition is created for business associates-"subcontractors"
- Physicians are not responsible for the actions of a BA subcontractor-the BA is!
- Physicians are still liable for the BA's conduct

PrivaPlan

Changes-Business Associates

- The new emphasis on “maintains” in the definition
- This gives rise to clarification regarding “conduits” vs. storage companies
- The analysis is whether the access is transient (as in a conduit) or persistent (as in storage company) nature of access
- The preamble clearly states that a data storage company that has access to protected health information (whether digital or hard copy) qualifies as a business associate, even if the entity does not view the information or only does so on a random or infrequent basis

PrivaPlan

Changes-Business Associates

- What does this mean?
- Document storage companies are clearly business associates
- As are data storage companies or data hosts such as:
  - A cloud based backup company
  - A commercial data center used either as a offsite backup firm or actually hosting your EHR!

PrivaPlan

Changes-Business Associates

- BA agreements will change! If you are using the PrivaPlan BAA template the impact is modest
- Physicians have until September 23, 2014 to bring all their BA agreements into conformance with the new rules. BA agreements that have not been renewed or modified between March 26, 2013 and September 23, 2013 will be deemed compliant until the date the BA agreement is renewed or modified or until September 22, 2014, whichever is earlier

PrivaPlan

The Breach Notification Rule-IFR compliance

- When this was drafted by HHS the intent was to harmonize with the many State laws
- Key concepts-breach of unsecured data and notification requirements
- The HITECH Act provides specific guidance for handling notification in case of a breach of "Unsecured PHI" that has been or is reasonably believed to have been:
  - Accessed
  - Acquired
  - Disclosed

PrivaPlan

Breach Notification continued

- HITECH and the Breach Rule introduces the term "unsecured PHI" where most State law describes this as "unencrypted computerized personal information"; HITECH maintains the integrity of the definition of PHI
- The Rule supports the principle of unsecured as relating to unencrypted data
- It provides guidance on how to render PHI "unusable, unreadable, or indecipherable to unauthorized individuals. This also incorporates a reference to NIST guidelines

PrivaPlan

Breach Notification continued

- HITECH notes data is vulnerable in multiple states such as
  - Data in motion
  - Data at rest
  - Data in use
  - Data disposed

Thus the Breach Notification Rule improves on the HIPAA Security rule by specifying these data states

PrivaPlan

Breach Notification continued

- The Rule states encryption and destruction are sufficient to secure PHI
- MOST IMPORTANTLY, the Rule APPLIES TO PAPER FORMS OF PHI!!!! That is, paper PHI can be breached if it is discarded and not properly destroyed
- The NIST guidelines reference use of cross cut shredding or similar ways to render a very small particle size (1X5 mm or 3/32 inch security screen)

PrivaPlan

Breach Notification continued

- Discovery begins on the first day which the breach is known either by you or your business associate!
- You are now required to notify individuals of any security breaches *promptly and without delay and* within 60 calendar days of discovery
- You bear the burden of proof that notification was completed
- This means detailed procedures for notification and good documentation when notification is done

PrivaPlan

Breach Notification continued

- Required methods of notification include:
  - Written notification (first-class mail) – E-mail if preference by the individual
  - If insufficient contact information to provide written notification and >10 individuals affected, then:
    - notification on your company website or another type of notification on company website
    - Some form of notice in major print should be posted
    - Immediately notify the Secretary, Health and Human Services if more than 500 individuals are affected
    - If fewer than 500 individuals are affected you can submit an annual log to the Secretary

PrivaPlan

Breach Notification continued

- DHHS will post breach information on their website; of course this could have a major effect on reputation
- Entities must provide a notice to prominent media outlets within a State or jurisdiction if the breach affects more than 500 residents of such State or jurisdiction – This could mean multiple notices being posted!
- Again, the Breach notification provision requires *detailed procedures!*

PrivaPlan

Breach-prevention is worth…

- We believe it is safer to encrypt data in the first place and thus prevent the costly notification requirement
- When it comes to HIT and EHRs beware—not all vendor systems sufficiently support encryption!
- Inventory your shredders and shredding procedures
- This is a good time to do another PHI inventory and use/disclosure flow diagram so you can also identify areas of vulnerability and remediate those

PrivaPlan

Handling a Breach-Practical Steps

- If you suspect a breach you must act quickly
- There are a number of investigative steps to take to determine if the incident is actually a breach
  - There are some initial steps
  - Determining if a breach of unsecured PHI occurred; this includes establishing a) a breach occurred and b) the data breached was unsecured PHI
  - If a breach occurred, was it to an "excepted party or circumstance". For example an unintentional acquisition by a member or your workforce.

PrivaPlan

Breach Notification continued

- If the breach was not to an excepted party, conducting a risk assessment to determine if the use or disclosure compromises the security or privacy of PHI, if a violation of the HIPAA Privacy rule occurred, and if the breach poses significant risk of financial, reputational, or other harm to the individual.
- If the breach was a Privacy violation and there is significant risk of harm, determine the type and amount of PHI and determine if the breach has been already mitigated.
- Essentially this means conducting an investigation and risk analysis!

PrivaPlan

Breach Notification continued

- Who made the impermissible use or to whom was the PHI impermissibly disclosed?
- Did the covered entity take immediate steps to mitigate an impermissible use or disclosure?
- Was the impermissibly disclosed PHI returned prior to access for an improper purpose?
- What type and how much PHI was involved?

PrivaPlan

Omnibus changes

- FINAL RULE AMENDS THE DEFINITION OF BREACH AT 45 CF 164.402
- KEY CONCEPT-HARM IS REPLACED BY THE CONCEPT OF THE RISK THAT PHI WAS COMPROMISED.." .....we have removed the harm standard and modified the risk assessment to focus more objectively on the risk that the protected health information has been compromised.'

PrivaPlan

Omnibus changes-Risk Assessment

- (1) The nature and extent of PHI involved;
- (2) The unauthorized person who used the PHI or to whom the disclosure was made;
- (3) Whether PHI was actually acquired or viewed; and
- (4) The extent to which the risk to PHI has been mitigated (*e.g.*, assurances from trusted third-parties that the information was destroyed).

PrivaPlan

Omnibus changes-Risk Assessment

- HHS includes not just unauthorized access to PHI, but also impermissible uses by knowledgeable insiders as a breach requiring an assessment.
- Breach is not limited to electronic personal information as some identity theft laws but pertains to any PHI

PrivaPlan

Omnibus changes-Risk Assessment

- An impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised
- Breach notification is necessary in all situations except those in which the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised (or one of the other exceptions to the definition of breach applies).

PrivaPlan

Omnibus changes-Risk Assessment

- Thus, breach notification is not required under the final rule if a covered entity or business associate, as applicable, demonstrates through a risk assessment that there is a low probability that the protected health information has been compromised, rather than demonstrate that there is no significant risk of harm to the individual as was provided under the interim final rule.

PrivaPlan

Omnibus changes-Risk Assessment

- The statute acknowledges, by including a specific definition of breach and identifying exceptions to this definition, as well as by providing that an unauthorized acquisition, access, use, or disclosure of protected health information must compromise the security or privacy of such information to be a breach, that there are several situations in which unauthorized acquisition, access, use, or disclosure of protected health information is so inconsequential that it does not warrant notification.

PrivaPlan

Omnibus changes-Risk Assessment

- The preamble even gives a common example:
  - For example, if a covered entity misdirects a fax containing protected health information to the wrong physician practice, and upon receipt, the receiving physician calls the covered entity to say he has received the fax in error and has destroyed it, the covered entity may be able to demonstrate after performing a risk assessment that there is a low risk that the protected health information has been compromised.

PrivaPlan

Omnibus changes-Risk Assessment

- As a result, instead of assessing the risk of harm to the individual, covered entities and business associates must assess the probability that the protected health information has been compromised based on a risk assessment that considers at least the following factors: (1) the nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification; (2) the unauthorized person who used the protected health information or to whom the disclosure was made;

PrivaPlan

Omnibus changes-Risk Assessment

- (3) whether the protected health information was actually acquired or viewed; and (4) the extent to which the risk to the protected health information has been mitigated.

Omnibus changes-Risk Assessment

Preamble states:

"As we have modified and incorporated the factors that must be considered when performing a risk assessment into the regulatory text, covered entities and business associates should examine their policies to ensure that when evaluating the risk of an impermissible use or disclosure they ***consider all of the required factors."***

Omnibus changes-Risk Assessment

"If an evaluation of the factors discussed above fails to demonstrate that there is a low probability that the protected health information has been compromised, breach notification is required. We do note, however, that a covered entity or business associate has the discretion to provide the required notifications following an impermissible use or disclosure of protected health information without performing a risk assessment. "

PrivaPlan

Omnibus changes-Notification

- "In response to those commenters who urged that we allow breach notices to be provided orally or via telephone to individuals receiving highly confidential treatment services where the individual has requested to receive communications in such a manner, we note that the HITECH Act specifically refers to "written" notice to be provided to individuals."

PrivaPlan

Omnibus changes-Notification

- "…in the limited circumstances in which an individual has agreed only to receive communications from a covered health care provider orally or by telephone, the provider is permitted under the Rule to telephone the individual to request and have the individual pick up their written breach notice from the provider directly. "

PrivaPlan

Omnibus changes-Notification

- "…In cases in which the individual does not agree or wish to travel to the provider to pick up the written breach notice, the health care provider should provide all of the information in the breach notice over the phone to the individual, document that it has done so, and the Department will exercise enforcement discretion in such cases with respect to the "written notice" requirement. "
- Document the "affirmative request of the patient"!

PrivaPlan

Enforcement

- The new rules clarify the three penalty tiers as follows:
- Lowest tier – cases in which the physician did not and reasonably could not know of the breach
- Intermediate tier – cases in which the physician "knew, or by exercising reasonable diligence would have known" of the violation, but the physician did not act with willful neglect
- Highest tier – cases in which the physician "acted with willful neglect"
-

PrivaPlan

Enforcement

- HHS must conduct a formal investigation and impose civil monetary penalties in cases involving willful neglect, and is now free to provide PHI to other government agencies for enforcement activities. The assessment of penalties must be based on five principal factors:
- (1) the nature and extent of the violation, including the number of individuals affected
- (2) the nature and extent of the harm resulting from the violation, including reputational harm
- (3) the history and extent of prior compliance

PrivaPlan

Enforcement

- (4) the financial condition of the covered entity or business associate
- (5) such other matters as justice may require. The number of violations may be based on the number of individuals affected or by the number of days of non-compliance.
- The rules further clarifies that the 30 day cure period begins when the physician knew or should have known of the violation.

PrivaPlan

Summary-What are your next steps?

- Updated Privacy, Security and Breach Notification policies and procedures (and in some cases new workflows and forms in the medical practice);
- Notice of Privacy Practices; and
- Business Associate Agreement revisions-in some cases analyzing if there are entities (such as an ePrescribing gateway or HIE) you need a BA with
- Workforce training

PrivaPlan

Summary-Resources

- PrivaPlan HIPAA Privacy and Security Toolkit-in many cases our forms are already adequate! The ToolKit will be revised in the coming months
- You may be eligible for a CORHIO sponsored toolkit!

PrivaPlan

Q & A

- Individual Questions?

PrivaPlan

Contact information

David Ginsberg
dginsberg@privaplan.com
1-877-218-7707