Chapter 5

Where Are We With HIPAA/HITECH? A Recap, Bright Spots and The Future

Final HIPAA Megarule: What's Changed, and a Guide to Complying for Providers

Clinton R. Mikel, Esq.
The Health Law Partners

Final HIPAA Megarule: What's Changed, and a Guide to Complying for Providers

By: ***Clinton R. Mikel, Esq.***

Complying with the HIPAA Megarule Checklist

1. Conduct a "Gap" Analysis/Overall Assessment of Current HIPAA Privacy/Security Compliance
2. Revise Notice of Privacy Practices and Replace Old Copies of the Same
3. Generally Revise, Implement, and Operationalize Policies, Procedures, and Forms Affected by the HIPAA Megarule
    a. **Federal Breach Notification and Breach Risk Assessment**. Update Policies/Procedures (Utilize Both Old and New Risk Assessment Guidance)
    b. **New "Paid-In-Full Insurer Restriction" Requirements**. Update Policies/Procedures on Patient Requested Restrictions and Revise Patient Request for Restrictions Forms
    c. **Fundraising**. Update Policies/Procedures Related to Fundraising
    d. **Research Authorizations**. Update Policies/Procedures Related to Research Authorizations, Update Research Authorization Forms (Optional)
    e. **New Access to Electronic PHI Requirements**. Update Policies/Procedures Related to Patient Access to PHI, Update Notice of Privacy Practices, and Update Patient Request for Access Forms
    f. **Marketing**. Update Policies/Procedures Related to Marketing Utilizing PHI, Update Marketing Patient Authorization Form
    g. **Sale**. Create Policies/Procedures Regarding Sale of PHI, Create Patient Sale of PHI Authorization Form
    h. **Decedent's PHI**. Update Policies/Procedures re: a Decedent's PHI
    i. **Immunization Records**. Create Policies/Procedures Regarding Disclosing Immunization Records
4. Revise Business Associate Agreement Template and Begin Replacing Old BAAs
5. Assess Who Might Now Be a Business Associate That Was Not Previously; Obtain BAAs From New Business Associates
6. Evaluate and Change Current Relationships that May be Implicated By "Marketing" and "Sales" Prohibitions
7. Promptly Identify and Correct Potential HIPAA Violations, In Order to Preserve Defense Against CMPs
8. Train/Re-Train All Staff Regarding HIPAA. Particular Training Focus Should be Given to Staff Whose Job Functions are Affected by Changes to the HIPAA Megarule

Key Dates

Jan 25, 2013 – Publication Date

March 26, 2013 – Effective Date

September 23, 2013 – Compliance Date

September 22, 2014 – Compliance Date for Grandfathered Business Associate Agreements

The Office for Civil Rights of the U.S. Department of Health & Human Services ("**OCR**") recently issued its long-awaited final regulations modifying the Health Insurance Portability and Accountability Act ("**HIPAA**") privacy, security, enforcement, and breach notification rules (the "**HIPAA Megarule**").[1] The HIPAA Megarule is a combination of regulations finalizing four sets of proposed or interim final rules that had been released since 2009's Health Information Technology for Economic and Clinical Health Act (the "**HITECH Act**"), as well as incorporating other changes required by the HITECH Act, and changes made by OCR under its regulatory authority.

I. Overview

The HIPAA Megarule addresses, among other things, five major topics:

1. Numerous revisions to the HIPAA privacy and security rules;
2. Substantial strengthening of the HIPAA enforcement rule and incorporating an increased monetary penalty tiered structure;
3. Incorporating and clarifying the HITECH Act's direct regulation of "business associates" and their "subcontractors";
4. Significant revisions to the breach notification rule; and
5. Modifications to the HIPAA privacy rule required by the Genetic Information Nondiscrimination Act.

The HIPAA Megarule will become effective on March 26, 2013, and compliance will be required by September 23, 2013.

II. This Chapter

This Chapter focuses on what covered entity ***health care providers*** need to know regarding the new changes to HIPAA contained in the new HIPAA Megarule. Though the topics covered in this Chapter are equally applicable to group health plans, insurers, HMOs, and business associates, this Chapter does not cover several additional HIPAA Megarule changes that are primarily of interest to these types of entities.

The Chapter summarizes the major HIPAA Megarule ***changes*** and attempts to detail steps that health care providers should take to ensure that they are in compliance with the HIPAA Megarule's changes.

---

1 *See* U.S. Department of Health and Human Services, 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, 78 *Fed. Reg.* 5566 (January 25, 2013), available at: http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf, which amends HIPAA, as mandated by the HITECH Act.

See also the ABA's Redline of the Final HIPAA Megarule, available to Health Law Section members for free at: http://www.americanbar.org/content/dam/aba/administrative/healthlaw/aba_health_law_hipaa_regs_for_redlining.pdf.

Note that the HIPAA Megarule does not address the accounting for disclosures requirement in section 13405 of the HITECH Act, which is the subject of a separate proposed rule published on May 31, 2011, at 76 FR 31426, or the penalty distribution methodology requirement in section 13410(c) of the HITECH Act, which will be the subject of a future rulemaking.

III. Your First Steps

To begin, health care providers should conduct a "gap" analysis, and otherwise perform an overall assessment of their current HIPAA Privacy/Security Compliance. This Chapter assumes that the provider has an appropriate baseline of HIPAA compliance, including having appropriate and required HIPAA Privacy and Security policies (which will, in turn, need to be updated for the HIPAA Megarule's changes). As such, as a baseline, providers should conduct a HIPAA Compliance Audit with an experienced health care attorney or compliance officer to assess whether they were in compliance with HIPAA before the new Megarule.

Importantly, providers need to ensure that they have appropriately conducted a HIPAA Security Rule Risk Analysis.[2] In short summation, a Security Rule Risk Analysis requires that the provider:

1. Evaluate how they receive, create, have access to, store, maintain, transmit, and use and disclose protected health information ("**PHI**");
2. Evaluate their administrative, physical, and technical safeguards with respect to the same, with the goals of:
    a. Ensuring the confidentiality, integrity, and availability of all PHI;
    b. Protecting against any reasonably anticipated threats or hazards to the security or integrity of such PHI;
    c. Protecting against any reasonably anticipated uses or disclosures of such PHI that are not permitted or required under HIPAA; and
    d. Ensuring that the provider's workforce is aware of and compliant with HIPAA;
3. Based on the evaluations above:
    a. ***Implement*** certain HIPAA enumerated "Required" security specifications; and
    b. Make a determination whether to implement certain HIPAA enumerated "Addressable" security specifications. If the "Addressable" specification is neither reasonable nor appropriate, the provider does not have to implement the same, but they are required to ***document their finding***, and implement an equivalent alternative measure if doing so is reasonable and appropriate (or document why an alternative measure is not reasonable or appropriate). If the "Addressable" security specification is reasonable and appropriate, however, the provider must implement the same; and
4. Scrupulously document all of the above.

Over the past several years, OCR officials have repeatedly stated that a failure to conduct and implement the findings of a HIPAA Security Rule Risk Analysis is one of the most common HIPAA problems, and, incidentally, is one of the least forgivable. Not surprisingly, after the OCR conducted its most recent covered entity HIPAA compliance audits, it cited Security Rule Risk Analysis failures as one of its most frequent findings. Intuitively, this makes sense. The Security Rule Risk Analysis provides a roadmap for a provider to safeguard their PHI—without the roadmap, there is no way for the provider to know where their risk areas are and their compliance efforts should be focused.

---

2 *See* 45 C.F.R. §§ 164.302 -164.318, which is generally referred to as the "HIPAA Security Rule" or the "HIPAA Security Standards".

IV. Required Changes to Notices of Privacy Practices[3]

The HIPAA Megarule requires modifications to a covered entity's notice of privacy practices by September 23, 2013. Providers must update their notices of privacy practices to include explanations regarding certain changes to patient's rights under the HIPAA Megarule, as well as changes to HIPAA's privacy rights.

In particular, the HIPAA Megarule requires the revised notice of privacy practices to include:[4]

- A description of the following uses and disclosures which ***require*** a patient authorization:
  - Most uses and disclosures of psychotherapy notes (if recorded by a covered entity);
  - Uses and disclosures of PHI for marketing purposes, including subsidized treatment communications; and Disclosures that constitute a sale of PHI;
- A statement that other uses and disclosures not described in the revised notice of privacy practices will not be made without the patient's authorization;
- A statement that the patient may revoke their authorizations;
- An explanation that the entity must agree to certain restrictions on its disclosures of PHI to health plans if the individual has paid out of pocket in full;
- If applicable and desired, a statement that the covered entity can contact the patient for fundraising purposes, and an explanation that they have the right to opt-out of fundraising communications;
- Notices of privacy practices may need to be updated to describe the patient's right to access PHI in an electronic form and format; and
- A statement that the covered entity is required to notify affected individuals following a breach of unsecured PHI.

Providers should do the following with respect to their notice of privacy practices:

- Make revisions to their notices of privacy practices (noting the revision/effective date). Providers should ensure that their notice accurately describes their ***actual*** day-to-day privacy practices;
- Replace all previous versions of the notice (website, physical location postings, and new patient distribution copies);
- Make the revised notices available to patients upon request (there is no requirement to distribute the new notice of privacy practices to patients who received the prior version); and
- Retain copies of the previous version of their notice of privacy practices, and of any written acknowledgements by patients of receipt of the same.

---

3 *See* regulatory commentary at 78 Fed. Reg. at 5623 *et seq.*; regulations at 45 C.F.R. § 164.520.

4 The HIPAA Megarule includes other required notice of privacy practice changes – the changes which are not summarized herein will not typically be applicable to treating providers, but are rather applicable to group health plans, insurers, HMOs, and the like.

Additionally, providers may delete the portions of their notice of privacy practices regarding use of PHI for appointment reminders and to discuss treatment alternatives.

V. Impact Related to Business Associate Relationships[5]

The HIPAA Megarule clarifies/affirms that business associates and their subcontractors who use PHI in performing their duties are directly liable for complying with the HIPAA security rule requirements, and certain provisions of the HIPAA privacy rule.

The HIPAA Megarule also clarifies/affirms that a covered entity may be liable for a business associates' acts or omissions if the business associate is an "agent" and is acting within the scope of their agency, as determined by the federal common law of agency, including if there are provisions in the business associate agreement ("**BAA**") contract whereby the covered entity has contractually controlled the actions of the business associate. This serves as a reminder for providers to use appropriate diligence in selecting their business associates, and also that they should likewise exercise caution when making determinations as to the level of control they wish to assert over their business associates.

Most importantly for providers, however, is that the HIPAA Megarule broadened the definition of who/what is considered to be a "business associate" relationship. These revisions to the HIPAA Megarule are significant. Providers should assess their relationships to determine who might now be considered a "business associate", in light of the expanded definition, since it is likely that their practice will be required to enter into business associate agreements with vendors who were not previously "business associates". The definition expands upon the previous "business associate" definition, by adding the following:

- Entities that transmit and need routine access to PHI (e.g., health information organizations, e-prescribing gateways, and others).
- Personal health record vendors who serve covered entities.
- A person or entity that creates, receives, ***maintains***, or transmits PHI on behalf of a covered entity. The addition of the word "maintains" recognizes that entities that maintain PHI on behalf of a covered entity, such as physical storage facilities or companies that store electronic PHI in the cloud, are business associates of the covered entity even if they do not access or view the PHI, unless they are truly mere "conduits", which are narrowly excepted from the definition of "business associate".

These revisions are significant and likely will require covered entities to enter into business associate agreements with additional contractors. For example, the following entities which were, in many instances, not business associates, are now directly regulated business associates under the HIPAA Megarule: (a) patient safety organizations; (b) data storage vendors—both cloud and physical; (c) data transmission organizations; (d) e-prescribing gateways; and (e) personal health records vendors. The HIPAA Megarule will also require changes to providers' BAA contracts. New BAAs must contain provisions that:

- Require that the business associate comply with the Security Rule obligations for electronic PHI and report breaches of unsecured PHI to the covered entity;
- Require business associates that carry out any part of a covered entity's obligation under the Privacy Rule to comply with the Privacy Rule with respect to that activity; and
- Require business associates that use subcontractors to enter into agreements with all such subcontractors that comply with the requirements for BAAs, and restricts the subcontractor from using/disclosing PHI in a manner that would not be permissible to the business associate.

5 *See* regulatory commentary at 78 Fed. Reg. at 5591 *et seq.*, 5598 *et seq.*, and 5570 *et seq.*; regulations at 45 C.F.R. §§ 160.103, 164.308(b), 164.502(a), (b) and (e), and 164.504(e).

- It is important to note that there is explicitly no obligation on the ***provider*** to contract with the subcontractor entities. The HIPAA Megarule is clear that it is the business associate's obligation to contract with subcontractors.

Additionally, covered entities are no longer required to notify OCR if they become aware of a material breach by a business associate that is not amenable to cure (unless the same constitutes a Breach of Unsecured PHI).

The OCR has released a new HIPAA Megarule compliant model BAA template, which can be accessed at: http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html.

A. Next Steps

Providers should review their existing BAAs—if they were updated to comply with the HITECH rules, it is possible (though not certain) that they comply with the HIPAA Megarule. If a prior BAA does not comply with the HIPAA Megarule, and the provider entered into the BAA on or before January 25, 2013, the provider must amend the BAA by the earlier of: (i) when the BAA is modified or renewed (excluding "evergreen" type auto-renewals); or (ii) September 22, 2014.

If a prior BAA does not comply with the HIPAA Megarule, and the provider entered into the BAA after January 25, 2013, the provider must amend the BAA by the earlier of: (i) when the BAA is modified or renewed (excluding "evergreen" type auto-renewals); or (ii) September 23, 2013.

Providers should ensure that all new contracts include a Megarule updated BAA, and put in place a process for replacing old BAAs by the deadlines noted above.

VI. Changes to Breach Notification Rule[6]

For nearly 3 years, providers have had to implement the breach notification regulations mandated by the HITECH Act (the "**Breach Notification Rule**") in the manner set forth in the August 24, 2009, interim final HITECH Act rules regarding breach notifications (the "**IFR**").[7] By way of brief background, the Breach Notification Rule requires covered entities to disclose to both patients and the government when there are specific kinds of security breaches involving an unauthorized use or disclosure of unsecured patient information. The HIPAA Megarule made two primary changes to the Breach Notification Rule regulations, but otherwise largely leaves the IFR intact,[8] including leaving the three enumerated exclusions from the Breach definition in place.[9]

6 *See* regulatory commentary at 78 Fed. Reg. at 5638 *et seq.*; regulations at 45 C.F.R. §§ 164.400 – 164.414.

7 *See* 74 Fed. Reg. 42740 (August 24, 2009).

8 Note, however, that there are still several pages of regulatory commentary in the HIPAA Megarule regarding the untouched requirements of the IFR that provide valuable insight for interpreting the Breach Notification Rules from the IFR. In particular, OCR "clarifies" provisions of the Breach Rules, including:

- When a breach is "discovered";
- Timeliness and methods of notification;
- Content of the breach notice;
- How covered entities acting as business associates should respond to a breach;
- When notice is given but it is undeliverable;
- Clarifies covered entity and media obligations for required large-scale Breach media reports; and
- Clarifies that every Breach of any size carries with it the potential for OCR enforcement and penalties, both for the Breach and for the Privacy Rule violation, as well as by possibly triggering further scrutiny for the provider.

9 *See* 45 C.F.R. § 164.402. The definition of "Breach" specifically excludes situations involving "Unsecured

First, and possibly most importantly, the HIPAA Megarule established that there is a ***presumption*** that ***any*** unauthorized use or disclosure of Unsecured PHI is a "***Breach***".

Second, since the publication of the IFR in 2009, stakeholders have eagerly speculated as to what, if any, changes would be made to its "risk of harm" standard, which allowed providers to avoid notification if they determined that the unauthorized use or disclosure "poses a ***significant risk of financial, reputational, or other harm to the individual***". The HIPAA Megarule purports to remove the IFR's "harm standard", and replace its "subjectivity" with a more "objective" and detailed standard of whether the PHI has been "compromised".

Thus, combining the two changes, under the HIPAA Megarule, ***any*** situation involving an impermissible access, acquisition, use or disclosure of PHI is ***presumed*** to be a breach unless the covered entity is able to demonstrate that there:

> ***"is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:***
>
> (i) ***The nature*** and extent ***of the protected health information involved***, including the types of identifiers and the likelihood of re-identification;
>
> (ii) ***The unauthorized person who used the protected health information or to whom the disclosure was made;***
>
> (iii) Whether the protected health information was actually acquired or viewed; and
>
> (iv) ***The extent to which the risk to the protected health information has been mitigated.***"

It remains to be seen whether the revisions to the Breach Notification Rule represent a material shift in policy or will routinely change the outcome of the breach/notification determination of providers. Interested parties should continue to monitor developments.

Protected Health Information", and also the following enumerated categories:

(i) Any ***unintentional*** acquisition, ***access, or use*** of protected health information ***by a workforce member*** or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use ***was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under subpart E of this part [the Privacy Rule].***

(ii) Any ***inadvertent disclosure by a person who is authorized*** to access protected health information at a covered entity or business associate ***to another person authorized to access*** protected health information ***at the same covered entity or business associate***, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure ***is not further used or disclosed in a manner not permitted under subpart E of this part [the Privacy Rule].***

(iii) ***A disclosure*** of protected health information ***where a covered entity or business associate has a good faith belief*** that an unauthorized person to whom the disclosure was made ***would not reasonably have been able to retain such information...***
(Emphasis Added).

It is this author's opinion, however, that the changes to the Breach Notification Rule are ultimately minor, at least with respect to the outcome of the "Breach or No-Breach" analysis that most providers will reach when they conduct their risk assessment. This interpretation has been given support by several regulatory comments issued within the HIPAA Megarule, and by public speaking engagements by officials from the OCR. For example, on February 22, 2013, the Executive Director of OCR indicated his agreement with this analysis in a speech given to the American Bar Association's Health Law Section at their Emerging Medical Issues Conference. In that speech, Mr. Leon Rodriguez indicated that he believes that for 98% of providers who are correctly complying with the Breach Notification Rule, the breach/no-breach outcome, and their decision trees for reaching the breach/no-breach conclusion, will not be significantly impacted by the final HIPAA Megarule, since in most cases the decisional factors are going to work the same way.

Nevertheless, the OCR has promised to issue additional guidance to aid covered entities and business associates in performing risk assessments with respect to frequently occurring scenarios. It is possible that the OCR will use such future guidance to influence the risk assessment process, either strengthening, loosening, or continuing to maintain the status quo as to the Breach/notification determination.

A. Next Steps

In any event, providers should update their federal Breach notification policies to reflect the HIPAA Megarule changes regarding the breach presumption and factors to be used in the risk assessment, and should scrupulously document any breach risk assessment they undertake using guidance from both the IFR and the HIPAA Megarule. Any risk assessment undertaken should be thorough, completed in good faith, and have reasonable conclusions. Note, however, that providers have discretion to provide breach notifications without performing the risk assessment.

VII. Requests for Restrictions[10]

Covered entities are not normally required to agree if a patient requests restrictions related to a use or disclosure of their PHI that would otherwise be allowed under HIPAA. The HITECH Act created an exception for certain healthcare services for which the patient pays out-of-pocket in full. The HIPAA Megarule implements this requirement, and ***requires*** covered entities ***to*** agree to restrict disclosures of a patient's PHI to an insurer if the service is paid for in full by the patient and certain other criteria are met.

Covered entities ***must*** agree to restrict disclosures of PHI if all of the following conditions are met (the "**Paid-in-Full Insurer Restriction**"):

- The disclosure is for payment or healthcare operations purposes;
- The disclosure is not otherwise required by law; and
- The PHI restricted pertains solely to a healthcare item or service for which the individual, or someone on the individual's behalf (other than the health plan), has paid the covered entity in full.

Note again the narrowness of the Paid-in-Full Insurer Restriction, particularly that if the conditions above are met, ***it does not mean that the entire medical record is subject to the restriction***. The only PHI restricted by the Paid-in-Full Insurer Restriction is the PHI that pertains solely to the item or service for which the individual paid in-full.

---

10 *See* regulatory commentary at 78 Fed. Reg. at 5626 *et seq.*; regulations at 45 C.F.R. § 164.522(a).

Covered entities do not need to create separate medical records or segregate PHI subject to the Paid-In-Full Insurer Restriction. It is required, however, that they have ***some methodology to flag or to identify the portions of the medical record that are restricted*** to ensure that the restricted information is not inadvertently sent or made accessible to the health plan for payment or healthcare operations purposes.

The HIPAA Megarule and its commentary address several other issues of note related to the Paid-In-Full Insurer Restriction. In particular, providers will find guidance related to complying with the Paid-in-Full Insurer Restriction when there have been bundled services (providers must counsel patients regarding the impact of the restriction on bundled services), payment is dishonored (in cases of dishonored payments, providers must make reasonable attempts to resolve payment issues with patient prior to disclosing PHI to the health plan, and, alternatively, a provider may choose to require payment in full at the time the restriction is requested to completely avoid payment issues), or follow-up care is obtained. The Megarule/commentary clarifies that there is no provider obligation to notify downstream providers of the Paid-In-Full Insurer Restriction, and that the Paid-In-Full Insurer Restriction trumps HMO contractual requirements. Finally, providers may include previously restricted PHI when billing health plans for follow-up treatment, to the extent that including such PHI is required to support medical necessity of follow-up care and the patient does not request the restriction/pay out-of-pocket for the follow-up care.

A. Next Steps

Providers should do the following to address compliance with the Paid-In-Full Insurer Restriction requirements:

- Revise policies and procedures to comply with the Paid-In-Full Insurer Restriction;
  - In particular, providers may wish to choose to require payment in full at the time the Paid-In-Full Insurer Restriction is requested to avoid payment issues;
- Revise their Patient Requests for Restrictions form to incorporate the Paid-In-Full Insurer Restriction Requirements;
- Evaluate processes and systems that will be affected by the Paid-In-Full Insurer Restriction, including electronic systems that may need to be updated to ensure that restricted information is not disclosed to, and health plans are not billed for, items or services subject to a Paid-In-Full Insurer Restriction; and
- Identify employees and contractors whose job functions will be affected by the Paid-In-Full Insurer Restriction and ensure that they are: (i) given the HIPAA Megarule's guidance regarding the same; and (ii) properly trained in implementing and protecting restricted PHI.

VIII. Limits on Marketing and Sale of PHI[11]

The HIPAA Megarule contains additional specificity regarding HIPAA's marketing and sale of PHI restrictions.

Covered entities will now generally, with exceptions, be prohibited from using or disclosing PHI for marketing/sale purposes without the patient's express special authorization for the same. Notably, as further described below, there are technical requirements applicable to what must be included in a "marketing authorization" (if Financial Remuneration is involved) and in a "sale authorization".

11 *See* regulatory commentary at 78 Fed. Reg. at 5592 *et seq., and* 5603 *et seq.*; regulations at 45 C.F.R. §§ 164.501, and 164.508.

Both the marketing and sales prohibitions include a new concept/definition of "**Financial Remuneration**", which is defined as direct or indirect payment from or on behalf of a third party whose product or service is being described. The HIPAA Megarule's commentary notes that non-financial benefits, such as in-kind benefits provided in exchange for making a communication about a product or service, ***are not*** Financial Remuneration.

A. Marketing

Under the HIPAA Megarule, any use or disclosure of PHI for "marketing" purposes requires patient authorization, except as noted below. "**Marketing**" is broadly defined as any treatment or healthcare operations communications to individuals about health-related products or services. However, the "marketing" definition excludes certain enumerated situations, and thus, uses and disclosures of PHI that meet the following criteria are allowed without obtaining patient authorization (if the use/disclosure is otherwise allowed under HIPAA):

- If the covered entity ***receives Financial Remuneration*** in exchange for making the communication, they may still do the following without it being considered "marketing", or requiring patient authorization, in the following instances:
  - Providers may make face-to-face communications to the patient, and provide promotional gifts of nominal value to the patient, without obtaining patient authorization
  - Relating to drugs and biologics, if the following conditions are met:
    - The Financial Remuneration is reasonably related to the costs associated with making the communication (labor, supplies, postage); and
    - The communication is to provide refill reminders or to send out other communications about a drug or biologic currently prescribed for the patient (including information about generic substitutes or instructions for taking the drug).
- If the covered entity ***does not*** receive Financial Remuneration in exchange for making the communication, in addition to the types of communications allowed above, a number of other communications are allowed and are not considered "marketing", including communications for purposes of providing treatment, case management, care coordination, recommending alternative treatments/providers, or describing health-related products or services provided by the covered entity.

Any other use or disclosure of PHI for "marketing" purposes is prohibited (whether or not Financial Remuneration is involved) without obtaining patient authorization. If the marketing involves Financial Remuneration, the patient authorization, in addition to all other HIPAA authorization requirements, must state that Financial Remuneration is involved.

B. Sales

Likewise, the HIPAA Megarule prohibits the sale of PHI without specific sale-related patient authorization, with certain exceptions. A "**sale of PHI**" occurs if a covered entity or a business associate directly or indirectly receives Financial Remuneration ***or non-financial remuneration*** in exchange for disclosing PHI to a third party. However, as with the definition of "marketing," the "sale of PHI" definition excludes certain enumerated items, and thus, the uses and disclosures of PHI that meet the following criteria are allowed without obtaining patient authorization (if the use/disclosure is otherwise allowed under HIPAA):

- Public health activities;
- Research (where the remuneration is limited to a reasonable cost-based fee);
- Treatment and payment purposes;
- The sale, transfer, merger or consolidation of all or part of a covered entity; or
- Though not truly "sales" of PHI, remuneration is also expressly permitted in connection with certain other transactions, including:
  - Covered Entities may pay business associates for activities that the business associate undertakes on behalf of a covered entity without those payments being considered a sale of PHI (but note that the payment is from the covered entity to the business associate);
    - Similar transactions between business associates and subcontractors are also permitted.
  - Providing PHI to the individual who is the subject of the information;
  - Provision of PHI as required by law; and
  - Other exchanges consistent with HIPAA where the only remuneration received by the covered entity or business associate is reasonable and covers the cost of preparing and transmitting the PHI, or if information is transferred for a fee expressly permitted by another law.

Any other sale of PHI for is prohibited without obtaining patient authorization. In addition to all other HIPAA authorization requirements, a patient authorization for the sale of PHI must state that the disclosure will result in remuneration to the covered entity.

C. *Next Steps*

Providers will need to evaluate their current relationships to determine whether they meet the "marketing" or "sales" definitions under the HIPAA Megarule, and, if so, will need to comply with the revised prohibitions by amending the relationships, terminating the relationships, or obtaining special patient authorizations for the sale/marketing. Further, providers will need to update their HIPAA policies and procedures related to uses and disclosures involving the marketing of PHI, and will need to create policies and procedures regarding the sale of PHI.

Providers will also need to update their patient marketing authorization forms, and create a sale of PHI patient authorization form. The marketing authorization must disclose that financial remuneration is received from a third party and state that the individual may revoke the authorization at any time. The sale of PHI authorization must state that the disclosure will result in financial remuneration to the covered entity.

IX. Changes to Patient Access to PHI Rights[12]

A. *Access to and Sending Electronic PHI*

The HIPAA Megarule provides that, if a patient requests PHI that is maintained electronically in a designated record set, the covered entity must provide them with electronic access in the form and format they have requested, if the information is readily producible in such format. If the information is not readily producible in that format, it must be given in a readable electronic form and format (e.g., PDF, word document, image file, access to secure EMR portal) as mutually agreed by the covered entity and individual. A hard copy may be provided if the individual rejects any of the offered electronic formats.

The HIPAA Megarule also addresses what a provider should do in situations where they maintain a medical record in mixed media (*e.g.*, paper documentation and EMR), that the provider does not have to use the patient's flash drive or other external media device if there are security concerns, and that if a patient requests that their medical record be sent via unencrypted email the provider must advise them of the risk that the information could be read by a third party.

The HIPAA Megarule also requires that, if a patient requests that PHI be sent directly to a third party, the covered entity must send the information to that third party if the individual signs a written request that clearly identifies the third party. Covered entities must implement policies and procedures to verify the identity of any person requesting PHI and implement reasonable safeguards to protect the information disclosed.

B. *Fees*

The HIPAA Megarule changes and clarifies what reasonable, cost-based fees the practice can charge for the patient's access to their PHI, including labor costs for copying PHI, whether in paper or electronic form. Providers should be aware of these changes, which are not summarized here, since most states have laws that preempt HIPAA in this regard and impose lower cost limits. If, however, a provider is not in such a state, they will need to revise their policies and procedures regarding charging for access to PHI in light of the HIPAA Megarule.

C. *Response Time*

The HIPAA Megarule requires covered entities to generally respond to requests for access within 30 days, with a maximum of 60 days in extraordinary cases when the provider has given the patient written notice of the delay. Previously, HIPAA allowed for up to 90 days when PHI was maintained offsite. Providers should note that the Meaningful Use program contemplates much faster access than 30 days.

D. *Next Steps*

Providers will need to update their patient requests for access forms, and revise their policies and procedures regarding the same to reflect the HIPAA Megarule's changes.

---

12 *See* regulatory commentary at 78 Fed. Reg. at 5631 *et seq.*; regulations at 45 C.F.R. §§ 164.524.

X. Increased HIPAA Enforcement[13]

The HITECH Act drastically changed the enforcement landscape related to HIPAA. Since the passage of the HITECH Act, OCR has begun auditing providers, and has levied numerous ***hundred-thousand-dollar-plus***, and even ***million-dollar-plus***, penalties on providers (including smaller physician groups).

The HIPAA Megarule formalizes the HITECH Act requirements, and makes it clear that the OCR's recent ramp-up of HIPAA enforcement is not merely a passing trend. The new rules underscore that both covered entities and business associates must reassess and strengthen their HIPAA compliance, or face potential severe monetary consequences for their failure to do so.

A. *Investigations Triggered by Willful Neglect*

The HIPAA Megarule clarifies when OCR must conduct a larger-scale investigation of a complaint it receives. Under the Megarule, the Secretary "***will***" [i.e., must] "investigate any complaint . . . when a preliminary review of the facts indicates a possible violation due to willful neglect." The Secretary "***may***" initiate an investigation for all other complaints.

Similarly, the Secretary is directed to undertake a full HIPPA compliance review of a covered entity or business associate (as opposed to merely investigating the matter which was the subject of a complaint), "when a preliminary review of the facts indicates a possible violation due to willful neglect". The Secretary "***may***" conduct a compliance review in any other circumstance.

B. *Civil Monetary Penalties*

The HIPAA Megarule also clarifies a number of issues dealing with the imposition of Civil Monetary Penalties ("**CMPs**"). Under HITECH and the Megarule, penalties are imposed based on a tiered structure that considers the level of knowledge and the culpability of the violator. The Megarule establishes the following tiered structure:

1. **Did Not Know**. Violations where the covered entity or business associate did not know and, by exercising reasonable diligence, would not have known about the violation;
2. **Reasonable Cause**. Violations in which it is established that the violation was due to reasonable cause and not willful neglect:
3. **Willful Neglect—Corrected**. Violations that were the result of willful neglect, but are corrected within 30 days of when the violator knew or through exercise of reasonable diligence would have known, about the violation; and

---

13 *See* HIPAA Administrative Simplification: Enforcement; Interim Final Rule, 74 Fed. Reg. 56123 (October 30, 2009); Modifications to the HIPAA Privacy, Security, and Enforcement Rules Under the Health Information Technology for Economic and Clinical Health Act; Proposed Rule, 75 Fed. Reg. 40,867 (proposed July 14, 2010) (to be codified at 45 C.F.R. pts. 160 and 164).

See Megarule regulatory commentary at 78 Fed. Reg. at 5577 *et seq.*; regulations at 45 C.F.R. §§ 160.306(c)(2), 160.401, 160.402(c), and 160.408.

See regulatory commentary at 78 Fed. Reg. at 5638 *et seq.*; regulations at 45 C.F.R. §§ 164.400 – 164.414.

4. **Willful Neglect—Not Corrected**. Violations due to willful neglect that were not corrected in the 30-day period beginning on the first date the covered entity knew, or by exercising reasonable diligence should have known, about the violation.

The Megarule also provides minimum and maximum penalty amounts depending on the tier. It is important to point out, however, that the maximum penalty amount does not set a total cap on penalties, but rather sets a maximum for identical violations. Penalties could increase significantly if the covered entity or business associate has multiple different penalties/violations.

Violation Category	Each Violation	All Identical Violations per Calendar Year
Did Not Know	$100—$50,000	$1,500,000
Reasonable Cause	$1,000—$50,000	$1,500,000
Willful Neglect—Corrected	$10,000—$50,000	$1,500,000
Willful Neglect—Not Corrected	$50,000	$1,500,000

The Megarule includes a number of factors for the Secretary to consider when determining the amount of CMP fine to impose on a violator. The factors can be either mitigating or aggravating, and include:

a. The nature of the violation, including:
    1. The number of individuals affected; and
    2. The time period.
b. The nature and extent of the harm resulting from the violation:
    1. Whether there was physical harm;
    2. Financial harm; or
    3. Reputational harm; or
    4. Whether the violation hindered an individual's ability to obtain health care.
c. The history of compliance for the covered entity or business associate and whether:
    1. Current violations are the same or similar to previous violations
    2. Whether the violator has attempted to correct previous noncompliance
    3. How the violator has responded to technical assistance; and
    4. How has the violator responded to past complaints.
d. The financial condition of the violator:
    1. Did financial difficulties affect compliance;
    2. Will CMPs affect the violator's ability to continue providing or paying for health care; or
    3. The violator's size.
e. Other factors specific to the individual situation.

Overall, under the Megarule, how the Secretary calculates penalties is dependent on the specific nature of the violations and may be calculated based on a number of different factors. The

HIPAA Megarule allows the Secretary to waive, in whole or in part, any CMPs. Conversely, and importantly for providers, in a shift from the prior HIPAA law, the Megarule gives the Secretary to ability to impose CMPs ***without exhausting other informal resolution options***, particularly when violations are due to willful neglect.

C. *Defenses*

The HIPAA Megarule adds two affirmative defenses that limit the Secretary's ability to impose CMPs.

Under the Megarule, the Secretary may not impose CMPs if the covered entity or business associate can establish that the violation was:

1. Not due to willful neglect; and
2. Corrected during either:
   a. A 30-day period beginning the date the violation was discovered or would have been discovered through exercise of reasonable diligence; or
   b. An additional period the Secretary deems appropriate based on the nature and extent of the failure.

The Megarule also bars CMPs when the covered entity or business associate can establish that criminal penalties have already been imposed.

Beyond a thorough and robust compliance plan, covered entities and business associates that learn of violations, whether due to willful neglect or otherwise, should take immediate action to correct the violations. For those violations not due to willful neglect, a violator that begins work to correct the violation may be able to avoid the imposition of CMPs through the affirmative defense detailed above. However, even in cases where the violation was due to willful neglect, the violator may be able to limit the amount of CMP imposed through mitigating factors, and by promptly correcting the violation under the tiered structure of CMPs as discussed above.

XI. Research[14]

Under the HIPAA Megarule, researchers will now be able to combine multiple authorizations into a single document. This change will provide researchers with some flexibility in designing the authorization and will better align the requirements with the NIH/HHS research "Common Rule" and other research requirements.[15]

Although the HIPAA Megarule continues to contain a general prohibition on combining HIPAA authorization with other legal permissions into a so-called "compound authorization", the Megarule also creates an exception to this general prohibition, which allows researchers to combine HIPAA authorizations with "any other type of written permission" for the same research study. In practice, this will allow researchers to create a compound authorization, which will allow for a single form to: (a) authorize the use of PHI; (b) authorize the storage of information for future use (*e.g.*, a bio-specimen bank); and (c) give general consent for the patient to participate in the study itself.

---

14 *See* regulatory commentary at 78 Fed. Reg. at 5609 *et seq.*; regulations at 45 C.F.R. § 164.508(b)(3).

15 *See* 78 Fed. Reg. 5566, 5610-13 (January 25, 2013).

HIPAA also generally prohibits a covered entity from "conditioning" the patient's treatment on the patient signing a HIPAA authorization giving the provider greater use/disclosure rights. Thus, a provider may not refuse to treat a patient if the refusal is based on the patient being unwilling to authorize the provider to sell the patient's PHI. One general intuitive exception to this rule, however, is that covered entities can condition a patient participating in a "research" course of treatment on the patient authorizing them to use/disclose their PHI for research purposes. Previously, a permissible "conditioned" research HIPAA authorization (i.e., you must give this authorization in order to receive treatment) could not be combined with an "unconditioned" authorization for optional corollary activities. The HIPAA Megarule now allows for combining "conditioned" authorizations with "unconditioned" authorizations. In this scenario, the HIPAA Megarule requires that the authorization "sufficiently differentiate" the primary and corollary activities of a study, and allow study participants to "opt-in" to the corollary components (i.e., the "unconditioned" portion of the research). The "opt-in" for the optional corollary components may include check boxes authorizing both the conditional and unconditional components with a single signature. The OCR, however, expressly declined to allow researchers use an "opt-out" provision, as the agency believed such a provision could be seen as coercive and did not provide participants the "clear ability to authorize the optional research activity."

One exception to the ability to combine research authorizations is with regards to research involving the use or disclosure of psychotherapy notes. For this type of research, authorizations may only be combined with another authorization for the use or disclosure of psychotherapy notes.

The HIPAA Megarule also changes the rules regarding authorization for future disclosures of PHI for research purposes. Under the HIPAA Megarule, a research authorization is no longer required to merely describe a single specific study, but may instead describe multiple current and potential future studies, so long as the authorization includes each of the core elements and statements required elsewhere in HIPAA. More specifically, the authorization must "adequately describe such purposes such that it would be reasonable for the individual to expect that his or her protected health information could be used or disclosed for such future research."

A. Next Steps

Providers who conduct research should revise their policies and procedures, and should update their research authorization forms to the extent desired to allow for compound authorizations (including combining "conditional"/"unconditional" authorizations), and for future research uses/disclosures. The change in the rules regarding compound authorizations is not a requirement and does not affect ongoing studies that are already using multiple authorization forms. For new studies, this rule gives researchers and IRBs flexibility to design the authorization as they see fit, whether that includes a compound authorization form, or multiple authorization forms.

XII. Fundraising Activities[16]

The HIPAA Megarule grants new flexibility to covered entities who wish to use or disclose PHI for fundraising purposes. Previously, providers were only allowed to use/disclose an extremely limited subset of the patient's PHI (demographic information and dates of service) when conducting their fundraising operations. To use or disclose any of the patients' other PHI for fundraising purposes, health care entities had to obtain an authorization, which often proved impracticable and inappropriate.

The HIPAA Megarule modifies the fundraising rules to allow covered entities to more effectively target individuals for fundraising, while at the same time avoiding inappropriate solicitations to all individuals.

16 *See* regulatory commentary at 78 Fed. Reg. at 5618 *et seq.*; regulations at 45 C.F.R. § 164.514(f).

In addition to maintaining that it is permissible to use/disclose dates of service and demographic information for fundraising purposes, the HIPAA Megarule now allows use/disclosure of the following information:

- Department where the services were provided to that patient (e.g. cardiology, neurology, etc.);
- The treating physician;
- Outcome information (*i.e.*, to allow for filtering of fundraiser targeting to avoid sending such communications to poor-outcome patients); and
- Health insurance status.

The Megarule also clarifies that "demographic information" includes an individual's name, address, contact information, gender, and date of birth.

If a covered entity wishes to conduct fundraising operations, it is required to include a statement to this affect in its revised notice of privacy practices.

In addition, in the fundraising communication itself, the HIPAA Megarule requires that the patient be provided with a clear method for opting-out of any future fundraising communications. This opportunity to opt-out does not need to be given prior to fundraising communication being sent, but should accompany the first such communication and all fundraising communications thereafter. The opt-out must be a clear and conspicuous opportunity to opt-out of any further fundraising communications. The method for opting-out may not impose an undue burden.

If an individual has elected to opt-out, the covered entity may not make fundraising communications to that person. Nevertheless, the covered entity may provide a method by which opted-out individuals may opt back in to fundraising communications.

The OCR clarified that the limitations outlined above apply to all forms of fundraising communication—not just written.

A. *Next Steps*

Providers should do the following with respect to the new fundraising communication requirements:

- Strategically consider new fundraising options available utilizing the new data elements;
- Amend their notice of privacy practices to explicitly notify individuals that they may be contacted for the purpose of fundraising for the organization;
- Establish a clear method or means for individuals to opt-out of further fundraising communications. The method must not be unduly burdensome on individuals. OCR specifically suggests use of a toll-free number, an email address, or other similar mechanisms. Determining which opt-out method is most appropriate will often depend on the scope and size of the communication;
- Notify individuals in each communication of the adopted opt-out procedure. Individuals should also be assured that treatment or payment are not conditioned on receiving fundraising communications, and individuals may choose to opt-out of such communications;
- Establish a method by which individuals may later opt back in to receive future fundraising communications; and

- Maintain effective data management systems to timely track and flag individuals who have opted out to ensure they do not receive any additional fundraising communications.

XIII. Immunizations[17]

Covered entities will no longer be required to obtain a written authorization to share immunization records with schools in certain instances. The HIPAA Megarule now allows disclosure of proof of immunization records to a school ***without written authorizations*** if:

- The school is required by the State or other law to have proof of immunization prior to admitting the individual; and
- Either the parent/guardian or the individual (if an adult or emancipated minor) "agrees" to the disclosure (verbally or in writing).

Note that the "agreement" can be verbal and does not need to be in the form of a written authorization or otherwise be obtained from the parent/guardian, but the agreement must be documented by the covered entity in the patient's medical records.

Practically, this change allows a covered entity to obtain authorization from the parent/guardian over the phone, such as when a parent or guardian calls to request that immunization records be provided to a school. The provider merely needs to document the call/"agreement" in the patient's medical record, and forward on the immunization records to the school. Agreements are valid until revoked by the parent, guardian, or individual if the individual is an adult or emancipated minor. The OCR believes that this rule is flexible enough to accommodate state requirements that covered entities communicate immunization records directly with the school as the agreement does not need to be in any specific form.

A. *Next Steps*

Providers that receive requests for proof of immunization for an individual should create policies and procedures whereby the provider, before releasing proof of immunization, ascertains that:

- Such proof is required by the State or another law;
- The parent/guardian or the individual (if an adult or emancipated minor) agrees to the disclosure; and
- The agreement, which may be oral, is documented in the medical records by the provider.

XIV. Decedents[18]

Under the HIPAA Megarule, the health information of an individual who has been deceased for 50 years is not considered PHI and therefore not subject to HIPAA. Covered entities may continue, however, to treat this information as PHI, at their election. Note that this is ***not*** a requirement for the covered entity to maintain PHI for 50 years.

The rule also clarifies that a covered entity may release/disclose a deceased individual's PHI to a family member or close personal friend who was involved in the individual's healthcare, or payment for the

17 *See* regulatory commentary at 78 Fed. Reg. at 5616 *et seq.*; regulations at 45 C.F.R. § 164.512(b).

18 *See* regulatory commentary at 78 Fed. Reg. at 5613 *et seq.*; regulations at 45 C.F.R. §§ 164.502(f) and 164.510(b).

individual's healthcare, to the extent relevant to that involvement. However, disclosure to the family member or close friend is not permitted if the decedent made an express wish against such a disclosure prior to death.

A. *Next steps*

Providers will need to update their policies regarding handling of a decedent's PHI and disclosures to family members involved in their treatment or payment for treatment.

XV. Other Resources

Unfortunately, the changing HIPAA landscape is not occurring in a HIPAA-Megarule-vacuum. Instead, the law, and regulatory agency guidance on the law, is rapidly evolving. Thus, even though this Chapter has attempted to distill the critical aspects that a health care provider needs to know to comply with the HIPAA Megarule, it is not authoritative, and by the time publication occurs, it is highly likely that additional guidance will have been issued. Providers should monitor the OCR's website for future developments (http://www.hhs.gov/ocr/privacy/).

Illustrating the continuing evolution of the HIPAA law, in just the past few months, the OCR and other related regulatory agencies have released the following guidance of which providers should be aware:

1. New Tools to Educate Consumers and Providers about HIPAA Privacy and Security
    a. Consumer fact sheets regarding consumer rights under the HIPAA Privacy Rule:
        i. http://www.hhs.gov/ocr/privacy/hipaa/understanding/consumers
    b. New modules for health care providers on compliance with various aspects of the HIPAA Privacy and Security Rules, available at Medscape.org:
        i. Patient Privacy: A Guide for Providers
            1. http://www.medscape.org/viewarticle/781892?src=ocr
        ii. HIPAA and You: Building a Culture of Compliance
            1. http://www.medscape.org/viewarticle/762170?src=ocr
        iii. Examining Compliance with the HIPAA Privacy Rule
            1. http://www.medscape.org/viewarticle/763251?src=ocr
        iv. The Medscape modules offer free Continuing Medical Education (CME) credits for physicians and Continuing Education (CE) credits for health care professionals.
2. OCR Responses to a Shooting Tragedy
    a. Advance Notice of Proposed Rulemaking, HIPAA Privacy Rule and the National Instant Criminal Background Check System
        i. https://s3.amazonaws.com/public-inspection.federalregister.gov/2013-09602.pdf
        ii. Solicitation of public comments.
        iii. OCR had been told there are concerns in certain states as to whether HIPAA is a barrier to States' reporting the identities of individuals subject to a firearm purchasing "mental health prohibitor" to the National Instant Criminal Background Check System ("**NICS**"). OCR is considering creating an express permission in the HIPAA rules for reporting the relevant information to the NICS by those HIPAA covered entities responsible for involuntary commitments or the formal adjudications that would subject individuals to

the mental health prohibitor, or that are otherwise designated by the States to report to the NICS.

   b. OCR Letter re: Disclosures to Avert Threats to Health or Safety (January 2013)
      i. http://www.hhs.gov/ocr/office/lettertonationhcp.pdf
      ii. Reminds providers of HIPAA's standards for permissible disclosures to avert threats to health or safety
3. OCR Audit Program Protocol covers Privacy, Security, Breach Notification Rules (June 2012)
   a. Provides an important insight into what OCR is looking for when it audits providers for HIPAA compliance, as well as OCR's current thinking regarding best compliance practices
   b. http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/index.html
4. OCR Guidance on De-Identification of Health Information (November 2012)
   a. http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/De-identification/guidance.html
5. OCR Right to Access Memo (May 2012)
   a. http://www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/righttoaccessmemo.pdf
   b. Educates and reminds patients of their rights to access their medical records under HIPAA
6. NIST HIPAA Security Rule Toolkit (October 2011)
   a. http://scap.nist.gov/hipaa/
   b. Application to conduct assessment of HIPAA Security policies, procedures, plans and controls
7. Focus on Mobile Devices and Their HIPAA Risks
   a. OCR Guidance on Mobile Devices (December 2012)
      i. http://www.hhs.gov/news/press/2012pres/12/20121212a.html
   b. FTC Guide on Mobile Devices (February 2013)
      i. http://www.ftc.gov/os/2013/02/130201mobileprivacyreport.pdf
8. OCR Privacy and Security Tutorials on YouTube
   a. http://www.youtube.com/user/USGovHHSOCR
   b. Primarily focused on patient rights under HIPAA

XVI. Staff Training

After digesting this Chapter and how the HIPAA Megarule's changes affect their organization, providers should train/re-train their staff members regarding HIPAA, and document that the training was held as part of their HIPAA compliance efforts.

Particular emphasis should be given on training/educating staff members whose job functions or workflow will be impacted by the HIPAA Megarule's changes

XVII. Conclusion

The HIPAA Megarule underscores that covered entities must reassess and strengthen their HIPAA compliance, or face potential severe monetary consequences for their failure to do so. Though September 23, 2013, may seem like it is far away, the HIPAA Megarule is extensive and complex, and can seem like a "death by a thousand cuts". In order to achieve new-HIPAA Megarule compliance, providers should get started now by doing a "gap" analysis to see what they are missing from a HIPAA Privacy and Security Rule perspective, what must be revised, and otherwise conduct an overall assessment of the impact of the HIPAA Megarule on their practices. After doing so, and implementing the changes outlined in this Chapter, the provider should train/re-train their staff regarding HIPAA, and the changes set forth in the HIPAA Megarule.