



New HIPAA Rules: A Guide for Radiology Providers

Adrienne Dresevic, Esq and Clinton Mikel, Esq

The credit earned from the Quick Credit™ test accompanying this article may be applied to the AHRQ certified radiology administrator (CRA) communication & information management domain.



EXECUTIVE SUMMARY

- The Office for Civil Rights issued its long awaited final regulations modifying the HIPAA privacy, security, enforcement, and breach notification rules—the HIPAA Megarule.
- The new HIPAA rules will require revisions to Notice of Privacy Practices, changes to business associate agreements, revisions to HIPAA privacy and security policies and procedures, and an overall assessment of HIPAA compliance.
- The HIPAA Megarule formalizes the HITECH Act requirements, and makes it clear that the OCRs 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 HIPAA compliance.

The Office for Civil Rights (OCR) of the US Department of Health & Human Services recently issued its long awaited final regulations modifying the HIPAA privacy, security, enforcement, and breach notification rules (the HIPAA Megarule). The HIPAA Megarule is a combination of regulations finalizing four sets of proposed or interim final rules that had been released since 2009s HITECH Act, as well as incorporating other changes required by the HITECH Act, and changes made by OCR under its regulatory authority.

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 becomes effective March 26, 2013, and compliance will be required by September 23, 2013. Summarized below are highlights from the HIPAA Megarule that will be of particular interest to radiology providers. See Box 1 for recommended steps for compliance.

Required Changes to Notices of Privacy Practices

The HIPAA Megarule requires modifications to a covered entity's notice of privacy practices. Radiology 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*:

1. A description of the types of uses and disclosures that require an authorization (including, without limitation, certain types of "marketing"

*The HIPAA Megarule includes other required notice of privacy practice changes—the changes which are not summarized herein will not typically be applicable to radiology providers.

■ Box 1. Recommended Steps for Radiology Providers to Comply with the HIPAA Megarule

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. Revise policies and procedures affected by the HIPAA Megarule
4. Revise authorization forms
5. Revise business associate agreement template and begin replacing old BAAs
6. Assess who might now be a business associate who was not previously
7. Evaluate and change current relationships that may be implicated by marketing and sales prohibitions
8. Update Federal Breach Notification policies/procedures and utilize both old and new risk assessment guidance
9. Implement the new "Paid-In-Full Insurer Restriction" requirements
10. Implement new access to electronic PHI requirements, and update policies and procedures related to patient access to PHI
11. Train/retrain all staff regarding HIPAA – focus should be given to staff whose job functions are affected by changes to the HIPAA Megarule

and "sale" of protected health information [PHI]);

2. An explanation that the entity must agree to certain restrictions on its disclosures of PHI if the individual has paid out of pocket in full;
3. If applicable, an explanation that the individual has a right to opt out of fundraising communications; and
4. A statement that the covered entity is required to notify affected individuals following a breach of unsecured PHI.

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

1. Make revisions to their notices of privacy practices (noting the revision/effective date);
2. Replace all previous versions of the notice (website, physical location postings, and new patient distribution copies); and
3. Make the revised notices available to patients upon request.

Impact Related to Business Associates

The HIPAA Megarule broadened the definition of who is considered to be a "business associate." These revisions to the HIPAA Megarule are significant. Radiology 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 practices will be required to enter into business associate agreements with vendors who were not previously business associates. The expanded definition of "business associate" expands upon the previous definition by adding the following:

- Entities that transmit and need routine access to PHI (eg, 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.

The HIPAA Megarule will also require changes to radiology providers' business associate agreement contracts (BAA). 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.

If radiology providers have BAAs now in force, the existing agreements are grandfathered until September 22, 2014 to permit amendments to comply with the final regulations.

Changes to Breach Notification Rule

For nearly three years, radiology providers have had to implement the breach notification regulations mandated by

the HITECH Act (the Breach Rule) in the manner set forth in the August 24, 2009 interim final HITECH Act rules regarding breach notifications (the IFR). The Breach 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 Rule regulations.

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 IFRs 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 PHI has been compromised based on a risk assessment of at least the following factors:

- The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
- The unauthorized person who used the protected health information or to whom the disclosure was made;
- Whether the protected health information was actually acquired or viewed; and
- The extent to which the risk to the protected health information has been mitigated.

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

In any event, radiology providers should update their federal Breach notification policies to reflect the HIPAA Megarule changes, and should scrupulously document any risk assessment they undertake using guidance from both the IFR and the HIPAA Megarule.

Requests for Restrictions

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 patients’ 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 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.

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, radiology providers will find guidance in the rule related to complying with the Paid-in-Full Insurer Restriction where there have been bundled services, payment is dishonored (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. Furthermore, the rule/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.

Radiology 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;

- 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: Given the HIPAA Megarule's guidance regarding the same; and properly trained in implementing and protecting restricted PHI.

Limits on Marketing and Sale of PHI

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/sales purposes without the patient's express special authorization for the same. Notably, there are technical requirements applicable to what must be included in a "marketing authorization" (if financial remuneration is involved) and in a "sale authorization." 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.

Marketing

Under the HIPAA Megarule, any use or disclosure of PHI for marketing purposes requires patient authorization, except as subsequently noted. 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 for the use/disclosure, they may still do the following without it being considered marketing:
 - The financial remuneration is reasonably related to the costs associated with making the communication; 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, 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.

Providers may also still make face to face communications to the patient, and provide promotional gifts of nominal value to the patient, without obtaining patient authorization. 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.

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
- 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
 - 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 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.

Next Steps

Radiology 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, radiology providers will need to update their HIPAA policies and procedures related to uses and disclosures involving the sale or marketing of PHI.

Changes to Patient Access to PHI Rights

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 (eg, 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 radiology provider should do in situations where they maintain a medical record in mixed media (eg, 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 patients requests that their medical records 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 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.

Fees

The HIPAA Megarule changes and clarifies what reasonable, cost-based fees the radiology practice can charge for the patient's access to 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 and impose lower costs limits. If, however, a provider is not in such a state, they will need to revise policies and procedures regarding charging for access to PHI in light of the HIPAA Megarule.

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.

Next Steps

Radiology providers will need to update their requests for access forms, and revise their policies and procedures to reflect the HIPAA Megarule changes.

Increased HIPAA Enforcement

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 OCRs 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.

Other Changes

Additional notable items for radiology providers in the HIPAA Megarule which are not more fully summarized here include:

- Clarifying/affirming that a covered entity may be liable for violations due to the acts or omissions of their business associates who are "agents" and are acting within the scope of their agency, as determined by the federal common law of agency;
- Changes made regarding research, including:
 - Allowing research authorizations that are not study specific and authorize future research if certain conditions are met; and
 - Allowing for combining certain research authorizations that previously had to be separate, including combining "conditioned" authorizations (where receiving the treatment/research/procedure is conditioned on signing the authorization) and "unconditioned" authorizations if certain conditions are met.
- Changes making it easier to disclose immunization records to schools;
- Changes making business associates and their subcontractors who use PHI in performing their duties directly liable for complying with many of the HIPAA privacy and security rule requirements;
- New parameters governing fundraising activities; and
- Limit HIPAA protections for PHI to 50 years after the patient's death, and also make it easier to provide PHI to a recent decedent's relatives if certain conditions are met.

Conclusion

For radiology providers who are covered entities, the new HIPAA rules will, at a minimum, require revisions to their notice of privacy practices, authorization forms, business associate agreements, HIPAA privacy and security policies and procedures, and an overall assessment of their HIPAA compliance.

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. In order to achieve new HIPAA compliance, radiology 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. ☸

Adrienne Dresevic, Esq. is a founding shareholder of The Health Law Partners, PC. She graduated Magna Cum Laude from Wayne State University Law School. Ms. Dresevic practices in all areas of healthcare law and devotes a substantial portion of her practice to providing clients with counsel and analysis regarding compliance and Stark and fraud and abuse. She is a member of the American Health Lawyers Association, American Bar Association (ABA), State Bar of Michigan, and State Bar of New York. Ms. Dresevic is the Chair of the Publications Committee of the ABA Health Law Section. She also is the Chair of the ABA Fraud and Abuse Toolkit and has served as the Chair of the ABA eSource publication. Ms. Dresevic has written extensively and co-authors a column in AHRA's monthly newsletter Link. Ms. Dresevic can be contacted at adresevic@thehelp.com or by visiting www.thehelp.com.

Clinton Mikel, Esq., is a partner at The Health Law Partners, PC. He is a graduate of Cornell University and the University of Michigan Law School. Mr. Mikel practices in all areas of healthcare law and devotes a substantial portion of his practice to providing clients with counsel and analysis regarding HIPAA, telemedicine, compliance, Stark, and Anti-kickback. He is a member of the American Bar Association's Health Law Section, the American Health Lawyers Association, and the State Bars of California and Michigan. Mr. Mikel is the Vice Chair of the ABA's eHealth, Privacy & Security interest group, and is a Vice Chair of the ABA's Health Law Section Publications Committee. Mr. Mikel has written extensively, including, co-authoring a column in AHRA's monthly newsletter, Link. Mr. Mikel can be contacted at cmikel@thehelp.com or by visiting www.thehelp.com.



The Clear Choice for Safe & Accurate Patient Positioning

Pedia-Poser™ Pediatric Chair
Child immobilization safely & securely for C-Spine, chest, abdominal, airway AP, lateral, oblique views
Use for infants through 4 years
Rolling casters & high quality locking swivel base



Patient Positioning Step Platforms
Safe and accurate weight-bearing lateral X-rays of feet, ankles, and the lower leg
Multiple film slots, designed for use with bucky and fixed cassette



Step Platform for C-Arm Systems
Use your C-Arm System to deliver accurate weight-bearing lateral and AP foot images safely & efficiently
Perfectly matched to systems from Swissray, IMIX, IDC and others
Easily portable with high-quality lockable casters



CR & DR Panel Protection
Avoid expensive panel damage in weight-bearing imaging
Safe non-slip rubber floorgrrips
Unbreakable clear faceplate
Up to 750lb Capacity



Free shipping to mainland US locations!
Seeking U.S. and International Dealers and Resellers

734-645-2833 www.ClearImageDevices.com