

Information Privacy and Security

HIPAA and Beyond

YOU CAN DEMONSTRATE DUE DILIGENCE with the [HIPAA Privacy and Security rules](#), so you are all set, right?

Well, you are certainly in good shape, but guess what, there is more. Did you know about the privacy and security requirements in the [Medicare and Medicaid EHR Incentive Program Final Rule](#)? Did you know that these privacy and security requirements fit hand and glove with the HIPAA privacy and security mandates? Plus, there is crossover between the current HIPAA privacy and security requirements and the HITECH updates in the Office for Civil Rights (OCR) July 2010 Notice of Proposed Rule Making (NPRM). So let's take a look at the big picture.

THE EHR INCENTIVE PROGRAM PRIVACY AND SECURITY IMPACTS

The privacy and security objective and measure in the CMS final rule states:

Meaningful Use Stage 1 Objective.

Protect electronic health information created or maintained by the certified EHR technology through the implementation of appropriate technical capabilities.

Meaningful Use Stage 1 Measure.

Conduct or review a security risk analysis per 45 CFR 164.308 (a)(1) and implement security updates as necessary and correct identified security deficiencies as part of its risk management process.

The measure is to conduct or review your security risk analysis part of the HIPAA Security Rule Security Manage-

ment process. Remember, the HIPAA Security Rule was written and implemented in the environment of electronic administrative data exchange, and little clinical data electronic exchange; and in the environment of point-to-point exchange, from a single provider to a single health plan or provider to provider. In contrast, the healthcare environment now includes HIOs, [HIEs](#), [ACOs](#), ePrescribing gateways and [personal health records](#), where data exchanges are now one-to-many. In addition, there are different types of guardians of the information.

The [Office of National Coordination \(ONC\)](#) final rule has eight areas that are outlined for specific security risk analysis:

- Access control.

- Emergency access.
- Automatic log-off.
- Audit log.
- Integrity.
- Authentication.
- General encryption and encryption when exchanging electronic health information.
- Accounting of disclosures.

So even if your latest risk analysis was done recently, you will need to consider at least the eight areas outlined above again for the larger scope. All the areas outlined above are in the [HIPAA Security Rule](#) except for the requirements for accounting of disclosures which is found in the HIPAA Privacy Rule, and in HITECH with an expanded scope that includes all disclosures made from an electronic data base.

You need to remember that the mandates are from the incentive program regulations so while you will need to do an updated risk analysis you will also need to find capability in all these areas in your EHR system. For example, a certified EHR must provide you the ability to encrypt and decrypt electronic health information, thereby allowing you this capability if you want or require this functionality.

THE OCR NOTICE OF PROPOSED RULEMAKING (NPRM)

The OCR NPRM has a number of modifications and updates including modifications to the HIPAA privacy and security requirements that the HITECH Act has mandated, and modifications to privacy and security requirements from the Patient

POLICY AND LEGISLATION: INFORMATION PRIVACY AND SECURITY

Safety and Quarterly Improvement Act of 2005 (PSQIA). Yes, the feds have decided that if they are talking about privacy and security in one regulation they can bring in mandates from several laws. This is the first time that this had happened.

OCR is proposing a few modifications in this NPRM to conform the HIPAA Privacy Rule to provisions in the PSQIA. For example the definition of a business associate (BA) now includes a provision to include patient safety organizations. In other words a patient safety organization will now be a BA! As a BA, a patient safety organizations will be included in the HIPAA healthcare operations definition.

OCR has gotten an earful of the unintended consequences that disclosure of information of decedents have caused under the current HIPAA privacy rule; they are proposing a change in how long you must keep such records under HIPAA lock and key. You will now need to keep the data for 50 years under HIPAA lock and key, and then it would no longer be protected health information (PHI).

The ripple effects are both administrative and technical. On the technical side you will need to update your system(s) to hold a date of death, and then age the data and make it at the end of 50 years, as open to the public. If this proposal makes it to the final rule, you will also need to add dates of death to the records now on file and age the records, as the effective period will not be 50 years down the road. On the administrative side you will need to update your policies and procedures and training.

One more tricky issue within this NPRM is the ability for a patient to pay in full for medical care and services and then ask you not to report to their health plan, their insurer. Imagine a patient who uses your clinics for blood work, and then the oncology clinic for a bit, but this patient is finally hospitalized and you ask for payment when the original services and care are not on file with health plan. The health plan may ask why they should make payment for this care when there is no underlying diagnosis and the tests to reach the diagnosis.

What we have here is a federal regulation that is attempting to solve a social problem.

You, however, will need to think this area through so that you can shield this information in your electronic files from the health plans when they do claims management, and you will have to have an administrative process in place to deal with the situation of first cash payment and then health plan payment. It is suggested that you talk to your health plan partners now about this area to find a way to assure the health plan that the necessary spade work has been done prior to the ask for payment for the advanced care.

THE EXPANDED ENVIRONMENT – HIES AND ACOS

Now a quick note into the more complex environment—the industry is moving into the more fluid sharing of electronic information. There are four areas you need to begin to think about now:

- BAAs and other data sharing agreements.
- Consent management.
- Governance.
- Nationwide Health Information Network (NHIN) environment.

You are going to be asked to share data much more widely and many will want you to sign documents that will be similar to BAAs, but may be called data sharing agreements and will include other types of requirements. You will need to ask your legal department to be involved from the get go in this area. You will not want to own anyone else's liability.

You will also be asked to participate in consent management. This is partly controlled by federal law, but mostly controlled by multiple states law. Then there is patient preference and perception to take into consideration. There is no rhyme or reason in this area yet! The federal government, through the ONC committee, is working on this in the HIT Policy Committee Privacy and Security Tiger Team. They are discussing both the administrative issues and the technical issues at the same time.

There is a need for governance over the sharing of data across multiple enterprises. This governance can include the data sharing documents and the privacy and security policies and procedures specific to the larger environment. But it also includes how

organizations join an HIE and how HIEs can terminate an organization's membership when necessary.

Finally, there is yet another ONC policy committee governance. They are drafting governance specifically for the NHIN environment. If you are connected to an NHIN or plan to connect you need the requirements. If you are going to use NHIN Direct you may also need to work with these recommendations and rules when they are released.

FUTURE REGULATIONS

Finally, stay tuned! The Meaningful Use Stage 1 objective, measures, and related standards will move to Stage 2 by 2013 and Stage 2 by 2015. There are bound to be interrelated privacy and security issues, concerns, questions and complications.

CONCLUSION

When you conduct your next privacy or security assessment think about the ripple effects of all privacy and security requirements that you must implement for HIPAA, HITECH and related regulations. It is not just HIPAA anymore. The scope continues to grow! **JHIM**



Gerry Blass has over 35 years of experience in healthcare IT and compliance. Gerry provides IT and compliance consulting services and software that automates the management and

documentation of healthcare compliance activities. Gerry is the President & CEO of [Blass Consulting and Compliance LLC](#).



Susan A Miller, JD has 35 years of professional leadership experience spanning teaching, biochemistry research and law. Since 2002, Susan has provided independent consultation and legal

services to numerous healthcare entities including DHHS/CMS. Blass and Miller are co-founders of [HIPAA 411](#), a linked-in group.