HIPAA Compliance
Now Even More
Critical for Managed
Care Organizations

Increased Enforcement of the HIPAA Omnibus
Rule Beginning September 23, 2013 Makes
Stiff Penalties Possible for Managed Care
Organizations without Adequate Safeguards
for Protected Health Information

By Bob Chaput, CISSP, CIPP/US
CEO & Founder, Clearwater Compliance LLC
A BRAVE NEW WORLD

The stakes are being raised. As of September 23, 2013, the Office for Civil Rights (OCR) began enforcement of the HIPAA Omnibus Final Rule. As the U.S. Department of Health and Human Services (DHHS) Office for Civil Rights (OCR) Director Leon Rodriguez recently stated, the final Omnibus rule not only greatly enhances patient rights and protections but also “strengthens the ability of my office to vigorously enforce the HIPAA privacy and security protections, regardless of whether the information is being held by a health plan, a health care provider, or one of their business associates.”

Rodriguez has consistently stated that his office will aggressively pursue penalties for organizations that show “an ongoing failure to comply with HIPAA Privacy and Security Rules”.

Such organizations will likely be subject to “willful neglect” penalties, which carry a minimum of $50,000 per member/per day for each violation cited. Basically, willful neglect means the “conscious, intentional failure or reckless indifference” to the obligation to comply with the regulations. While a violation of a certain requirement once had a maximum fine of $25,000, it now carries a maximum of $1.5 million. Some attorneys have projected that an organization found in violation of the 22 standards related to the Security Rule could be fined as much as $33 million, for example.

Managed Care Organizations, including safety net health plans, are not exempted from this greatly increased focus on compliance. Safeguarding Protected Health Information (PHI) is a foundational requirement for all healthcare organizations, especially those directly responsible for the delivery of quality care, providing access to the right care and doing so in a timely manner. Safeguarding PHI is a matter of patient and member safety.

In addition to increased enforcement and significantly higher penalties, the HITECH Act mandates that the DHHS conduct periodic audits of both Covered Entities and Business Associates for compliance with HIPAA. The HITECH Act granted state attorneys general (SAG) jurisdiction to file civil suits on behalf of their citizens for HIPAA violations. A breach of protected health information is NOT required to trigger enforcement action; however, member or patient complaints, self-reported breaches and mandatory audits have been known to trigger lengthy and expensive investigations by the OCR resulting in
negotiated resolutions, settlement agreements, corrective action plans, formal monitoring program and/or negotiated penalties. Effective September 23, OCR is no longer required to seek an “informal resolution” to violations; in fact, OCR is required to investigate especially those cases involving “willful neglect”. With or without a breach, a Covered Entity (or a Business Associate) can be held accountable for failing to have properly complied with the regulatory requirements.

**MEMBER SAFETY AND COMPLIANCE CHALLENGES**

Despite the severe financial and business risks associated with noncompliance, there is an even more significant reason managed care organizations should be focused on HIPAA-HITECH compliance. Leading plans across the country have realized that delivering quality care, providing access for their members and ensuring care is delivered in a timely manner is directly dependent on the confidentiality, integrity and availability of members’ health information. The very same actions and processes that keep your organization in compliance with HIPAA-HITECH regulations also improve your ability to deliver on State Performance Domains of Care: Quality, Access and Timeliness.

Indeed, safeguarding PHI is not about complying with regulations. It is about quality of care, member safety and competitive advantage in a very dynamic healthcare marketplace. Today, it is a competitive differentiator in California in counties such as Los Angeles where the Medi-Cal Two-Plan Model is in place. The commercial health plan operating in that county has experienced one of the largest breaches of PHI in the country. When members have a choice, they will opt for health plans that have a better track record of protecting their very personal, intimate health information.

So where are health plans falling short? As a whole, Covered Entities have been consistently cited for inadequate or nonexistent:

- Risk analysis and risk management
- Security management programs
- Compliance gap assessment programs
- Contingency plans for the protection of PHI in case of loss or disaster
- Documented policies, procedures, and workforce training and sanctions
THREE MANAGED CARE COMPLIANCE CHALLENGES

Specifically, managed care organizations have three primary challenges to tackle head on as they attempt to shore up their compliance programs. A brief description of each follows:

1. Risk Analysis – A Foundational Element

Risk analysis is a core foundational step of any information security program and one required for HIPAA compliance, yet organizations largely have been found lacking in this area. In 2012, 68 percent of Covered Entities and 80 percent of Providers had adverse Risk Analysis findings when audited by the Office for Civil Rights. Since 2008, 100 percent of settled cases from OCR investigations cited bona fide Security Risk Analysis as a corrective action plan requirement.

If done the right way, a risk analysis will prepare your organization for a positive audit experience and identify exposures your organization must close to prevent a breach. It can better equip you to respond to an OCR investigation, or even to avoid an investigation altogether. A proper risk analysis is the foundation of a security program and offers a platform for effectively prioritizing risk management activities in a way that will best protect the health information of the people you serve and your organization’s reputation.

Meanwhile, average monthly complaints to DHHS for privacy violations have increased 42% since HITECH was enacted in 2009. In discussing the 2012 OCR Audit results, Susan McAndrew, Deputy Director for Health Information Privacy and Security for OCR, shared that noncompliance with the 78 requirements of the Privacy Rule were “sprinkled throughout the regulations.”

You see the headlines daily: DHHS penalizes yet another healthcare organization for a breach of protected health information (PHI) and/or failure to comply with specific regulatory requirements, garnering unwanted national media attention. What if you could drastically reduce – even prevent - data breaches, costly fines, penalties and permanent damage to your organization’s reputation?

Completing assessments of your compliance vis-à-vis each of these regulations is a critical step for all managed care organizations. In doing so, a cross-functional team should examine three key assessment / audit questions:

1. Does the organization have written policies and procedures or other appropriate documentation that demonstrates compliance with each implementation specification and requirement?
2. Is the organization abiding by / enforcing / practicing that which is documented in policies and procedures or other documentation?
3. Do the organization’s practices and/or enforcement of same, whether documented or not, represent reasonable and appropriate safeguards to comply with the implementation specification described above?

2. Security + Privacy + Breach Notification – A Balanced Approach

Although compliance with the requirements in the Security Rule, the Privacy Rule and the Breach Notification Rule is required of all Covered Entities, the results from the 2012 OCR HIPAA Audits reveal that the majority of noncompliance issues pertain to the HIPAA Security Rule. According to OCR, the top four security deficiencies identified during those audits were: failure to complete a risk analysis, user access and activity monitoring, contingency planning, authentication/integrity and media re-use and destruction. Details provided by OCR suggest that these issues of noncompliance could have been mitigated by better security documentation and/or adherence to strong security policies and procedures.
Not only are Business Associates now subject to the same Security Rule requirements as Covered Entities, in addition to relevant sections of the Privacy Rule and the HITECH Breach Notification Rule, but their subcontractors are as well. Any organizations that create, receive, maintain, or transmit PHI on behalf of a covered entity or another upstream business associate are considered Business Associates. Due to the extensive exposure many Business Associates have to PHI, the majority of responsibilities associated with Privacy, Security, and Breach Rules are relevant and applicable to them.

It is good news for managed care plans that Business Associates are statutorily obligated to comply with these regulations, but it does not automatically exonerate the plan from risks and liabilities that the Business Associate may create.

Now, managed care plans and other covered entities must obtain satisfactory assurance that their business associates will specifically comply with the HIPAA Security Rule to appropriately safeguard the information, documented through a written contract or agreement that meets the applicable regulatory requirements which have been expanded by the Omnibus Final Rule. Good news: HHS provides sample Business Associate Agreement provisions on its website. This newly acquired responsibility places a significant new burden on covered entities, particularly managed care organizations and others that have a wide variety of outsourced partners. Managed care plans may have dozens of vendors who create, receive, maintain or transmit PHI. In our work managed care plans, we have identified packaged software vendors, application development contractors, file / data storage companies, claims clearinghouses, web portal companies, Medicare HCC Coding Companies, call center software firms, document imaging companies, claims scrubbing companies, pharmacy benefits managers, cloud-storage providers and data analytics companies, among others.

Managed care plans need not only update their Business Associate Agreements; we strongly recommend that they take proactive steps to manage their Business Associates. These steps include, but need not be limited to:

1. Form a Cross-Functional Team
2. Inventory all Business Associates
3. Rank Order Business Associates According to Risk
4. Send an Initial Written Communication Asserting Commitment to Compliance and Expectations
5. Update all Business Associate Agreements According to Requirements- Consider Additional Contractual Requirements for High Risk BAs
6. Conduct a Business Associate Summit Meeting and Document Meeting Agenda, Attendees and Outcomes
7. Collaborate with Like Businesses - Assess Business Associates Once Where Possible
8. Implement an ongoing Business Associate Monitoring and Management Program
KEY STEPS TOWARD COMPLIANCE

Managed care plans should take the following recommended steps as soon as possible. **Thoroughly document each step** to best position your organization to demonstrate good faith effort and compliance.

1. Establish or update a Privacy and Security Risk Management & Governance Program. From a security standpoint, the program should incorporate focus on the implementation of “security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.”

2. Develop or update comprehensive HIPAA Privacy, Security, and Breach Notification Policies & Procedures. These procedures should cover all applicable standards and implementation specifications in the Privacy, Security and Breach Notification Rules.

3. Train employees and other workforce members on policies and procedures (at least annually and whenever revised) and clearly define the disciplinary consequences for non-compliance. Bear in mind that 93% of PHI breaches of more than 500 records, made public by DHHS, were caused by people. Only 7% were caused by IT incidents or hacking. Be sure to maintain accurate records of all training performed and sanctions applied.

4. Complete a bona fide HIPAA Security Risk Analysis. The HIPAA Security Rule defines this as “an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of electronic protected health information held by the entity.” Just an FYI, a Service Organization Control (SOC) 2 or 3 assessment/report does NOT constitute a bona fide HIPAA Security Risk Analysis. DHHS/OCR has issued explicit guidance on how to complete a bona fide risk analysis.

5. Establish or update a strong, proactive Business Associate Management Program. Execute an updated Business Associate agreement with any vendor that has access to your PHI by September 23rd, or later if your current contract meets certain requirements.

6. Conduct a HIPAA Security Evaluation. This compliance gap assessment, to ensure your Risk Management Program has addressed all applicable sections of the Security Rule, is required and is not the same as a HIPAA Security Risk Analysis.

7. Complete Privacy Rule and Breach Notification Rule compliance gap assessments. These assessments, to ensure your organization has addressed all applicable sections of the Privacy and Breach Rules, are recommended as good business practice as they will prepare you for OCR investigations and audits.

8. If your organization is involved in marketing, fundraising, research, underwriting, the sale of PHI or the PHI of deceased individuals, familiarize yourself with new Omnibus Final Rule requirements and update existing or develop new policies and procedures accordingly.

9. As a health plan, you are required to have a Notice of Privacy Practices (NPP), which must be reviewed and updated to reflect changes driven by the Omnibus Final Rule.

10. Document, act upon and maintain a “living, breathing” remediation plan to close any identified compliance gaps. This remediation plan will serve as additional evidence of your good faith effort to comply.
**Risk Management & Governance Program Development**

The following additional guidance may be helpful in creating or improving an organization-wide Risk Management Program.

- Identify and document where all the PHI “lives” in your organization—paper, electronic, or verbally communicated.
- Once you have identified all the “PHI homes”, create a matrix of all individuals or organization units within your business that have access to this information.
- Keep the HIPAA Minimum Necessary Requirement of the Privacy Rule in mind: limit PHI access to only those employees and other workforce members who need to see the information, and limit PHI use or disclosure to the minimum number of people necessary to accomplish the business purpose.
- Encrypt PHI that is stored or transmitted. Take note especially if it is stored on mobile devices. Train your workforce to always use secure, email or secure file transfer if transmitting PHI. Check to ensure any vendor creating, receiving, maintaining or transmitting PHI on your behalf is also encrypting.
- Make sure back-ups of PHI are encrypted and kept in a safe, secure place.
- When possible, keep PHI off laptops, tablets, smart phones, thumb drives, and other devices with a high risk of loss or theft. When not possible, encrypt, encrypt, encrypt!
- Develop and implement policies and procedures governing the use of employee-owned personal devices.
- Regularly monitor systems and traffic for unusual activity and monitor employees for adherence to PHI procedures.
- Document the process in your Risk Management Program to be followed if there is a security incident, privacy violation and/or breach of PHI. Ensure your Business Associate Agreements provide for timely notification to your Compliance Office of any incidents or breaches discovered by your vendors.
Tools to Help Managed Care Organizations Comply

No matter where you are on the road to compliance, the following resources can support your progress.

- Complete a [Covered Entity Omnibus ReadinessCheck™](#)
- Download a [HIPAA Risk Analysis Buyer’s Guide Checklist™](#)
- Participate in an intensive [HIPAA Compliance BootCamp™](#)
- Attend a [Live HIPAA-HITECH Web Event this Month](#)
- Download a white paper on [Risky Business: How to Conduct a Bona Fide HIPAA Security Risk Analysis](#)

For additional resources, visit [www.clearwatercompliance.com](http://www.clearwatercompliance.com)

---

Clearwater Compliance LLC

Our mission is simple: help you become and remain HIPAA-HITECH compliant! Clearwater Compliance, LLC, is all about and only about helping healthcare organizations and their service providers become and remain HIPAA-HITECH Compliant. Owned and operated by veteran, C-suite health care executives, Clearwater Compliance provides comprehensive, by-the-regs software and tools, risk management solutions, training, and professional services for small medical practices and healthcare startups to major healthcare systems, health plans and Fortune 100 companies. Since 2003, the company has served more than 350 organizations (including 100 hospitals).

To learn more about our company, visit: [www.ClearwaterCompliance.com](http://www.ClearwaterCompliance.com)

To learn more about our Risk Analysis solutions, visit: [www.HIPAASecurityRiskAnalysis.com](http://www.HIPAASecurityRiskAnalysis.com)

For more information on this White Paper please contact the following people:

Bob Chaput  
CEO & Founder  
615 656 4299  
800 704 3394  
bob.chaput@ClearwaterCompliance.com