Confusion Reigns in Determining HIPAA Requirements for Group Health Plans and their Plan Sponsors

By Mary Chaput, MBA, HCISPP, CIPP/US, CHP, CFO and CCO, Clearwater Compliance LLC

Special HIPAA Requirements for Group Health Plans and their Sponsors
Why Bother?

Group Health Plans (“GHPs”) have a lot of regulations with which to comply: ERISA (the Employee Retirement Income Security Act), MHPA (the Mental Health Parity Act), Newborns’ Act (the Newborns’ and Mothers’ Health Protection Act), WHCRA (the Women’s Health and Cancer Rights Act) and HIPAA (the Health Insurance Portability and Accountability Act). And while HIPAA isn’t new, there is certainly a renewed energy around enforcement. After all, fines, penalties and settlement dollars associated with HIPAA violations go back into the coffers of the Office for Civil Rights (“OCR”) for more enforcement activities in a year when government budgets are tight. Therefore, there is reason to believe that OCR will step up enforcement activities significantly in 2014 and beyond.

Penalties for non-compliance have increased with the enactment of the Omnibus Rule which details and implements significant changes called for in the 2009 HITECH Act. The HITECH Act mandates that the U.S. Department of Health and Human Services (DHHS) OCR conduct periodic audits of both Covered Entities and Business Associates for compliance with HIPAA. As Covered Entities, GHPs are subject to these same audits and other enforcement actions.

Following on the heels of the 2012 “compliance” audits (OCR acknowledged to be looking for weaknesses and best practices, with no punishments handed out for non-compliance), the 2014 OCR HIPAA Audits are expected to be about enforcement and disciplinary action. OCR officials have indicated that GHPs will be on the audit list again this year (as they were in 2012), along with their service providers. And with the newly available on-line complaint form, it’s easier than ever for someone to report to the Secretary of DHHS suspected violations of their, or anyone else’s, HIPAA privacy or security rights. This is a particularly sensitive allegation when employers and colleagues have access to an individual’s health information. State attorneys general are also granted jurisdiction to file civil suits on behalf of their citizens for HIPAA violations.

In sum, there are lots of ways to get into trouble if your GHP is not HIPAA compliant.
**Which GHPs Need to Comply?**

GHPs with less than 50 participants are not considered Covered Entities under HIPAA, and so are not required to comply with HIPAA regulations. All other GHPs, even fully-insured GHPs, will have certain obligations under the HIPAA Privacy and Security Rules and the HITECH Breach Notification Rule.

**What Penalties Are Involved?**

Not only are GHPs subject to the same criminal and civil penalties that other Covered Entities face for noncompliance, those penalties under the Omnibus Rule have dramatically increased orders of magnitude. Where there is “willful neglect”, penalties become very severe. While a violation of a certain requirement once had a maximum fine of $25,000, it now carries a maximum of $1.5 million. Typically, a breach involves many violations so the authorized penalties can easily amount to millions of dollars.

**Where there is “willful neglect”, penalties become very severe. While a violation of a certain requirement once had a maximum fine of $25,000, it now carries a maximum of $1.5 million.**

**What are GHP Responsibilities?**

Requirements will vary significantly from one GHP to the next. Careful review is required. Depending on the level of access to protected health information (“PHI”), GHPs must comply with various Privacy and Security Rule requirements as well as relevant sections of the HITECH Breach Notification Rule. The entire Security Rule may be applicable for those GHPs that create, receive, maintain or transmit electronic PHI of their covered members. Pertinent requirements in the Privacy Rule can include individual rights, uses and disclosures, notice of privacy practices and Administrative requirements depending on the services that the GHP provides and the information it shares with the plan sponsor.

For example, if the GHP provides health benefits solely through an insurance contract with a health insurance issuer or HMO (whether fully-insured or self-insured) and only provides (a) information to the plan sponsor on whether an individual is participating or has enrolled or disenrolled from the plan or (b) summary information for the purposes of obtaining premium bids or modifying the group health plan, the GHP will need to comply with only some of the Administrative requirements of the Privacy Rule (i.e. refraining from intimidating or retaliatory acts, no waiver of rights and documentation with respect to amended plan documents).

On the other hand, if a GHP discloses additional PHI, or allows a health insurance issuer or HMO to disclose PHI, to the plan sponsor, the GHP must first ensure that the plan documents restrict uses and disclosures of such information by the plan sponsor consistent with the requirements of HIPAA. Specifically, the plan documents must provide that, before any disclosure of PHI, the plan sponsor must certify that the plan documents:

- restrict uses and disclosures of PHI without authorization,
- ensure that any agents, including a subcontractor, to whom it provides PHI received from the group health plan agree to the same restrictions and conditions that apply to the plan sponsor
- provide for certain rights of individuals,
- make information available to the Secretary of DHHS for determining compliance,
- provide for the return or destruction of information received from the GHP and
- ensure adequate separation between the group health plan and plan sponsor.

In addition, the Group Health Plan must also comply with all Administrative Requirements of the Privacy Rule and provide a Notice of Privacy Practices to members of the GHP.
**Business Associates (“BA”) and BA Agreements**

Business Associates can include service providers who handle enrollment/disenrollment, eligibility, dental or vision plans, underwriting, claims management, collections, member advocacy, conducting or arranging for medical reviews, legal and auditing services. BA Agreements are required for all service providers with access to PHI and must contain a number of very specific provisions including language that imposes upon the BA the same restrictions and conditions with respect to PHI that apply to the plan sponsor.\(^{10}\)

A BA Agreement is not required for disclosures to a health plan sponsor by a group health plan, or by the health insurance issuer or HMO, if (a) the group health plan's documents have been amended to limit the disclosures or (b) the disclosure is limited to summary information or information on whether an individual is participating, or is enrolled or disenrolled in the plan.\(^{11}\)

**Key Areas of Emphasis for GHPs**

If your GHP or a service provider to your GHP provides any health information to your plan sponsor, it is recommended that you take the following steps immediately. Thoroughly document each step to position your organization to demonstrate compliance.

1. Establish a HIPAA Compliance Officer for your GHP and a HIPAA Oversight or Governance Committee to determine and oversee the establishment of an appropriate compliance program.

2. Identify and document where all PHI related to the GHP “lives” in your organization—paper, electronic, or oral—and its purpose.

3. Identify applicable HIPAA requirements based on the activities of the GHP and the health information shared with the plan sponsor and business associates.

4. Reduce the amount of PHI the plan sponsor sees or retains to the minimum necessary for the functions provided.

5. If adequate separation between the GHP and the plan sponsor is required, ensure that you document those workforce members with access to PHI, that access is restricted to the plan administration functions\(^{12}\) performed by the plan sponsor for the GHP and that an effective means for resolving noncompliance issues is implemented.

6. Conduct rigorous Privacy, Security and Breach Notification compliance assessments to determine gaps or weaknesses in applicable HIPAA requirements. Document and act on a remediation plan to close any identified compliance gaps.

7. Implement or update comprehensive HIPAA Privacy, Security, and Breach Notification Policies & Procedures to address any gaps in requirements.
8. Train employees on new and/or updated policies and procedures immediately (and thereafter at least annually) and clearly define the disciplinary consequences to employees if they fail to adhere. Maintain accurate records of all training performed.

9. If relevant, complete the bona fide HIPAA Security Risk Analysis required at 45 CFR 164.308(a)(1)(ii)(A).

10. Identify and risk rate current Business Associates; establish or update a proactive program to update, as needed, BA agreements and a monitoring program to ensure reasonable and appropriate safeguards are in place and privacy violations or security incidents are being promptly reported.

11. Review the plan documents for required changes and obtain required certifications from the plan sponsor.

12. If a Notice of Privacy Practices (NPP) is required, review and update for required changes.


**Tools to Help Group Health Plans Comply**

Whatever the state of your organization’s readiness for the enforcement of HIPAA Omnibus Rule, take advantage of resources available to ensure or strengthen compliance.

- Complete a [Clearwater Covered Entity Omnibus ReadinessCheck™](#)
- **Require your GHP Business Associates to complete a Clearwater Business Associate 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](#)

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-reg 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

To learn more about our Risk Analysis solutions, visit: 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

© 2014 Clearwater Compliance LLP. This article is intended for general information purposes only and should not be construed as legal advice or legal opinions on any specific facts or circumstances.
Endnotes

1 as defined in section 2791(a) of the Public Health Service Act

2 § 160.103 Definitions.

Group health plan (also see definition of Health plan in this section) means an employee welfare benefit plan (as defined in section 3(1) of the Employee Retirement Income and Security Act of 1974 (ERISA), 29 U.S.C. 1002(1)), including insured and self-insured plans, to the extent that the plan provides medical care (as defined in section 2791(a)(2) of the Public Health Service Act (PHS Act), 42 U.S.C. 300gg-91(a)(2)), including items and services paid for as medical care, to employees or their dependents directly or through insurance, reimbursement, or otherwise, that:

1. Has 50 or more participants (as defined in section 3(7) of ERISA, 29 U.S.C. 1002(7)); or
2. Is administered by an entity other than the employer that established and maintains the plan.

3 Title 45 Code of Federal Regulation Part 164 - http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&sid=16609cfc04f0ec2dc6f525ac8ecc98f&p=ecfr

4 defined as “conscious, intentional failure or reckless indifference to the obligation to comply”

5 § 164.504(a)Definitions. Summary health information means information, that may be individually identifiable health information, and:

1. That summarizes the claims history, claims expenses, or type of claims experienced by individuals for whom a plan sponsor has provided health benefits under a group health plan; and
2. From which the information described at §164.514(b)(2)(i) (Requirements for de-identification) has been deleted, except that the geographic information described in §164.514(b)(2)(i)(B) need only be aggregated to the level of a five digit zip code

6 § 164.530(k) Reduced Administrative requirements. Group Health Plans

To the extent that:
1. The group health plan provides health benefits solely through an insurance contract with a health insurance issuer or an HMO; and
2. The group health plan does not create or receive protected health information, except for:
   a. Summary health information as defined in §164.504(a); or
   b. Information on whether the individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan;

The group health plan is not subject to the standards or implementation specifications in paragraphs (a) personnel designations (b) training (c) safeguards (d) complaints (e) sanctions (f) mitigation or (i) policies and procedures.

However, the GHP is still subject to (g) refraining from intimidating or retaliatory acts (h) waiver of rights (j) documentation, but only with respect to plan documents amended in accordance with §164.504(f).

7 § 164.504 (f)(2)(ii) Requirements for Group Health Plan and (2) Requirements for plan documents.

8 § 164.530(k) provides that a Group Health Plan is not subject to the standards or implementation specifications in paragraphs (a) through (f) of 165.530 (a) personnel designations (b) training (c) safeguards (d) complaints (e) sanctions (f) mitigation (g) refraining from intimidating or retaliatory acts (h) waiver of rights (i) policies and procedures and (j) documentation) to the extent that:

1. The group health plan provides health benefits solely through an insurance contract with a health insurance issuer or an HMO; and
2. The group health plan does not create or receive protected health information, except for:
   a. Summary health information as defined in §164.504(a); or
   b. Information on whether the individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan.

9 § 164.504 (a) Notice of Privacy Practices (2)(ii) A group health plan that provides health benefits solely through an insurance contract with a health insurance issuer or HMO, and that creates or receives protected health information in addition to summary health information as defined in §164.504(a) or information on whether the individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan, must:
   (A) Maintain a notice under this section; and
   (B) Provide such notice upon request to any person. The provisions of paragraph (c)(1) of this section do not apply to such group health plan.

10 § 164.504(f)(2)(ii)(B) Ensure that any agents to whom it provides protected health information received from the group health plan agree to the same restrictions and conditions that apply to the plan sponsor with respect to such information;

11 § 160.103 (4) Business associate does not include (ii) A plan sponsor, with respect to disclosures by a group health plan (or by a health insurance issuer or HMO with respect to a group health plan) to the plan sponsor, to the extent that the requirements of § 164.504(f) of this subchapter apply and are met.

12 § 164.504(a) Definitions. Plan administration functions means administration functions performed by the plan sponsor of a group health plan on behalf of the group health plan and excludes functions performed by the plan sponsor in connection with any other benefit or benefit plan of the plan sponsor.