The Granade Law Firm

DEDICATED TO COUNSELING THE HEALTH CARE INDUSTRY REGARDING PRIVACY AND SECURITY LAWS

Phyllis F. Granade

pgranade@granadelaw.com

www.granadelaw.com

Atlanta, Georgia

(678) 705-2507

March 6, 2013

HIPAA Final Rule 2013
Overview of Key Changes that Require Action

NOTE: This Overview is written primarily for Covered Entities that are hospital systems or other health care providers, with an emphasis on large health systems.

REMINDERS:

1. Rule issued: January 25, 2013
2. Effective date: March 26, 2013
3. Compliance deadline (generally): September 23, 2013
4. Compliance deadline for amending BAAs signed prior to January 25th: September 23, 2014

REQUIRED ACTIONS include, but are not limited to:

1) Update the following Policies and Procedures:

a) Data Breach Policy and Toolkit

b) Business Associates Policy

c) Research (changes to "compound authorizations" in research context)

d) Notice of Privacy Practices

i) Entities that will need updated NPPs:

(1) Hospitals, ASCs, Practices, Health Plans

ii) NPPs should be updated to include HIPAA Final Rule's changes concerning:

(1) Right to notification of a HIPAA breach involving individuals PHI

(2) Fundraising (right to opt out, instructions to do so)

(3) Authorization required for most uses/disclosures of psychotherapy notes

(4) Right to request information not be disclosed to health plan if paid in full out of pocket (NPP already contains this language, I believe)

(5) Marketing for remuneration (authorization required in most cases)

(6) Access rights to electronic copy of PHI in form requested, if reasonable

(7) Sale of PHI (authorization required)

(8) Genetic information is PHI (i.e., Genetic Information Nondiscrimination Act or GINA)

(9) Immunization disclosures to schools with parent/guardian verbal agreement

(10 Right to decedent information (e.g., for family treatment purposes, payment of bills)

e) Many definitions in Policies must change, including:

i) PHI (add genetic information)

ii) Business associate

iii) Breach

Phyllis F. Granade

pgranade@granadelaw.com

www.granadelaw.com

Atlanta, Georgia

(678) 705-2507

iv) Authorizations

v) Genetic information (new)

vi) New: Immunization as a permitted disclosure with verbal agreement

2) Implement new workforce member training re: changes in the regulations and your policies

3) Revise BAAs (yes, your organization may need more than one template):

a) Pro-Covered Entity template BAA to be used with vendors that are business associates (e.g., for hospitals, ASCs, physician practices, etc.)

b) Related entities contracting for or on behalf of owned/managed covered entities (i.e., BAA between corporate entity that is not a Covered Entity and its owned/operated Covered Entities)

c) Pro-Business Associate BAA template, if any entities act as business associates to covered entities or subcontractors of business associates. See item 4, below.

d) Security Agreement – include in your BAA or in a separate agreement the details of how your organization wants its vendors to protect PHI. For example, if a business associate maintains or transmits your organization's ePHI, what level of encryption must the vendor use?

4) Determine which of your organization's entities act as business associates (if any)

a) Identify entities, if any, that provide BA services **outside** the Covered Entity's enterprise

b) Pro-Business Associate template BAAs

i) Consider corporate veil discussions as it relates to Civil Monetary Penalties (CMPs). Keep the waters clean between the various related organizations; failure to do so could cause OCR to consider your organizations sufficiently related to breach the corporate veil, which may result in OCR increasing CMPs imposed.

ii) Adoption (and documentation) of appropriate Privacy and Security Policies and related workforce member training

c) Ensure your organization's BAA is adopted by your vendors. If your organization must use another entity's BAA, keep a "checklist" of terms to which your organization will not agree.

i) Example: In certain circumstances it is not worth doing business with a CE that insists on unreasonable provisions that subject your organization to unlimited liability, dangerous levels of liability, or that will immediately cause your organization to violate the BAA or the your own policies.

ii) Consider: Insurance for data breaches/cyber liability. Unlimited indemnification. Reimbursement of costs/expenses alternatives.

5) Entities that act as business associates must comply with the HIPAA Security Standards and applicable HIPAA Privacy Standards. Examples:

i) Conduct a written risk assessment in accordance with Security Standards

ii) Prepare written responsive risk management plan

(1) These are but two examples of the dozens of "implementation specifications" or actions that must be taken to comply with the Security Standards

(2) OCR is paying very close attention to completion of these requirements by CEs and BAs

Phyllis F. Granade

pgranade@granadelaw.com

www.granadelaw.com

Atlanta, Georgia

(678) 705-2507

iii) Create written policies and procedures in accordance with Security Standards

iv) Adopt appropriate policies and procedures regarding Privacy Standard compliance

v) Adopt template BAAs (consider a neutral or "friendly" BAA for use with your customers, and a more strict version (e.g., containing indemnification) another for use with your subcontractors

vi) Enter into BAAs with all subcontractors, maintain a BAA contract administration system

vii) Document compliance efforts in writing (including BAAs), retain for six years beyond last effective date of document