HIPAA BUSINESS ASSOCIATE AGREEMENT BEST PRACTICES: A COMPLIANCE SOLUTION FOR THE TICKING CLOCK AND THE DRACONIAN CIVIL AND CRIMINAL PENALTIES

January 23, 2014

I. Executive Summary I: The HIPAA Final Rule and the Enhanced Civil Fine Regime

The Health Insurance Portability and Accountability Act (HIPAA) Omnibus (final privacy) Rule (HIPAA Final Rule), published by the Department of Health and Human Services (HHS) on January 25, 2013 pursuant to the Health Information Technology for Economic and Clinical Health (HITECH) Act and the Genetic Information Nondiscrimination Act, imposed a short compliance deadline of September 23, 2013 on all Business Associate Agreements (BAAs) entered into after January 25, 2013. *Additionally, all new BAAs must be compliant now, post-January 25, 2013.* All BAAs entered into before January 25, 2013 must be updated and made compliant *by September 22, 2014*, and thousands of such agreements exist. The HIPAA Final Rule makes all HIPAA Covered Entities *and their Business Associates* (both defined below) *primarily and directly liable* for compliance. In the past, Business Associates were not primarily and directly liable. As a practical matter, all agreements by Covered Entities with third parties who electronically receive, process, store or retransmit a Covered Entity's patient protected health information (PHI) are BAAs, and must be reviewed and required BAA terms incorporated, customized and optimized for the particular business relationship involved, and the third parties are HIPAA - regulated Business Associates in that relationship. Moreover, audit and compliance programs must be in place on both the Covered Entity and Business Associate sides to make sure that the BAA provisions are actually complied with throughout the life of the agreement.

Among other changes, the HIPAA Final Rule changes the HIPAA Enforcement Rule to incorporate the increased, tiered civil money penalties and even criminal penalties provided by the HITECH Act. Those potential civil penalties are game-changers: *fines can go up to $50,000.00 per occurrence and $1,500,000.00 per section violation per year, even in cases when a Covered Entity did not know it was committing a HIPAA violation and would not have known even by exercising reasonable diligence.* Pre-HITECH HIPAA fines were generally a maximum of $100 per violation and an aggregate of $25,000.00 per year, which is why the healthcare/life sciences community has developed a culture of not taking them seriously. Additionally, because Business Associates were not directly and primarily liable under HIPAA before the HIPAA Final Rule, many service providers to Covered Entities do not even realize that they are HIPAA - regulated Business Associates. A full schedule of the civil fine schedule is appended to the end of this advisory as Appendix A. In the context of PHI delivered to an IT provider functioning as a Business Associate in breach of HIPAA, only 30 violations – something that could occur in an hour or in a day – could, at $50,000.00 each, reach the $1,500,000.00 aggregate for each of the Covered Entity and the Business Associate. *There are also criminal penalties that include up to one year of imprisonment even for violations done unknowingly or with reasonable cause to believe they were not violations.*

To call the new penalties draconian is an understatement; this is not the occasion for a nonchalant attitude towards regulatory compliance. HHS has made clear that it intends the new, civil penalties to have teeth. In July 2013, WellPoint agreed to pay HHS a $1.7 million penalty for HIPAA violations; in 2009, CVS Pharmacy

agreed to pay $2.25 million for PHI violations, and in 2012 alone, the Alaska Department of HHS paid a $1.7 million penalty, the Massachusetts Eye and Ear Infirmary settled a fine for $1.5 million and Blue Cross and Blue Shield of Tennessee settled a HIPAA fine for $1.5 million. In 2013, HHS settled a HIPAA breach case with Affinity Health Plan *for $1.2 million arising from disclosure of over 344,000 patients' PHI stored on leased photocopiers' memory when the photocopiers were returned to the leasing agent without erasing the PHI from their memory.* Another fine of $4.3 million was imposed on Cignet Health of Prince George's County, MD in 2011. In all, since July 2008, HHS has collected nearly $17 million in HIPAA fines and settlements thereof (so-called "resolution agreements").

II. Executive Summary II: A Compliance Solution

Many Covered Entities and Business Associates are under the impression that the dozen or so of HHS Office of Civil Rights (OCR) - required terms that are floating around the Internet on various forms are the BAAs that must be put in place between them. Actually, the BAAs are really the underlying service agreements between Covered Entities and Business Associates, or between Business Associates and their subcontractors, pursuant to which patient PHI is electronically transmitted, received, stored, or processed. A BAA may be a software license agreement, a data storage agreement, an insurance policy, a medical center's IT maintenance or billing services agreement, a HMO services or employment agreement or any of many other types of contract. The short-form sets of terms and conditions found on-line are not BAAs, they are only the minimum elements (with variable provisions) set forth in the Code of Federal Regulations - at 45 CFR 164.504(e) - that must be added to BAAs of whatever type, between whatever type of CE and BA, or BA and subcontractor. Call them the "HIPAA Final Rule Sample Terms."

HHS OCR did not intend the HIPAA Final Rule Sample Terms to become a short-form, catch-all compliance solution. The HHS OCR website states of the HIPAA Final Rule Sample Terms: "This is only sample language and use of these sample provisions is not required for compliance with the HIPAA Rules. The language may be changed to more accurately reflect business arrangements between a covered entity and business associate or business associate and subcontractor. In addition, these or similar provisions may be incorporated into an agreement for the provision of services between a covered entity and business associate or business associate and subcontractor, or they may be incorporated into a separate business associate agreement. These provisions address only concepts and requirements set forth in the HIPAA Privacy, Security, Breach Notification, and Enforcement Rules, and alone may not be sufficient to result in a binding contract under State law. They do not include many formalities and substantive provisions that may be required or typically included in a valid contract. Reliance on this sample may not be sufficient for compliance with State law."

It is important to realize that the HIPAA Final Rule Sample Terms are a minimum HHS OCR requirement for amending each BAA, and do not represent a thoughtful or prudent allocation of rights and responsibilities between each Covered Entity and each Business Associate, or each Business Associate and each subcontractor, in any given situation, nor do they take into account the provisions of the underlying BAA. For example, in any high-risk BAA (large amounts of PHI are being electronically transmitted pursuant to its terms), the HIPAA Final Rule Sample Terms, modified to be appropriate for that BAA, could be bolstered by terms providing for indemnification between the parties for the other's breaches, limitation of liability (either carving out from the

limitation damages subject to indemnification or not), choice of governing law, choice of forum for dispute resolution, confidentiality and others. Terms could also be added clarifying rights and responsibilities in the underlying BAA that had since been found to be ambiguous, or a source of contention or dissatisfaction between the parties. Combinations of these terms can be added to an appropriate (to the given BAA) version of the HIPAA Final Rule Sample Terms in a short addendum document to the underlying BAA. In some low-risk cases (small amounts of PHI being transmitted pursuant to the BAA), a "plain vanilla" stand-alone version of the HIPAA Final Rule Sample Terms simply making reference to the underlying BAA may be sufficient. In a third, small number of cases, in which the BAA is expiring, or is up for renewal, or was incompetently drafted originally, it may be prudent and cost-effective to prepare a full amendment and restatement of the BAA, incorporating the HIPAA Final Rule Sample Terms and others into the main body of the BAA.

III. Who is Affected?

For purposes of the HIPAA Final Rule, “Covered Entities” include:

- Health care providers (doctors, clinics, hospitals, medical centers, psychologists, dentists, chiropractors, nursing homes and pharmacies, when transmitting PHI in an electronic form in connection with a transaction governed by an HHS standard);

- Health plans (health insurance companies, health maintenance organizations, company health plans, Government programs that pay for health care, such as Medicare, Medicaid, military and veterans’ programs); and

- Health care clearinghouses (processors of nonstandard health information into a standard electronic or data format or vice versa).

“Business Associates” include:

- Health information organizations, e-prescribing gateways or other entities providing data transmission services to a Covered Entity and which requires routine access to the Covered Entity’s PHI. The definition is not exclusive, but excludes mere conduits of such data, such as telecommunications and Internet carriers;

- Entities offering personal health records on behalf of a Covered Entity;

- A subcontractor of a Business Associate handling PHI for that Business Associate other than as a mere conduit; and

- Anyone who creates, receives, maintains or transmits maintains PHI on behalf of a Covered Entity (including entities storing electronic PHI).

The HIPAA Final Rule, as stated, makes Business Associates directly and primarily liable for violations under the new civil monetary and criminal penalties, and establishes certain safe harbors in which Covered Entities are *not* acting as Business Associates, such as a health plan or insurer disclosing PHI to the plan's sponsor healthcare provider. Although the disclosing party is a Covered Entity, it is not, in that transaction, a Business Associate. A Business Associate may only use PHI subject to the limitations the HIPAA Privacy Rule imposes on Covered Entities. If the HIPAA Final Rule governs a Covered Entity's use of PHI, then it governs the Covered Entity's Business Associate receiving the PHI from it, and the Business Associate is directly and primarily liable. Business Associate direct liability for HIPAA Final Rule breaches include:

- Impermissible use or disclosure of PHI;
- Failure to notify a Covered Entity of breach;
- Failure to provide access to a copy of electronic PHI to the Covered Entity, the affected individual or his designee;
- Failure to disclose PHI when required by the HHS Secretary to investigate the Business Associate's HIPAA compliance;
- Failure to provide an accounting of disclosures;
- Failure to comply with the security rule; and
- Contractual liability under the BAA.

IV. Business Associate Agreements

As stated, HHS OCR has published minimum standards for BAAs. In terms of the BAA requirements published by HHS OCR, the following minimum requirements apply, *subject to HHS OCR's own statement, quoted above, that use of these terms does not constitute any kind of compliance safe harbor or sufficiency under State law:*

- BAAs must be written, executed agreements between Covered Entities and Business Associates and between Business Associates and their subcontractors;
- BAAs must establish the permitted and required uses and disclosures of PHI by the Business Associate;
- BAAs must provide that the Business Associate will not use or further disclose the information other than as required by the BAA or by other applicable law;
- BAAs must require the Business Associate to implement appropriate safeguards to prevent unauthorized use or disclosure of the PHI, including implementing requirements of the HIPAA Security Rule with

regard to electronic PHI;

- BAAs must require the Business Associate to report to the Covered Entity any use or disclosure of the PHI not provided for in the BAA, including incidents that constitute breaches of unsecured PHI;

- BAAs must require the Business Associate to disclose PHI as specified in the BAA to satisfy a Covered Entity's obligations for individuals' requests for copies of their PHI;

- If the BAA requires a Business Associate to carry out a Covered Entity's obligations under the HIPAA Privacy Rule, those requirements and obligations must be set forth explicitly and without ambiguity;

- BAAs must require the Business Associate to make available to HHS its internal practices, books and records relating to the use and disclosure of PHI received from, or created or received by, the Business Associate on behalf of the Covered Entity for purposes of determining the Covered Entity's compliance with the HIPAA Privacy Rule;

- BAAs must provide that at the termination of the BAA, the Business Associate, to the extent feasible, will return or destroy all PHI received from, or created or received by, the Business Associate on behalf of the Covered Entity;

- BAAs must require the Business Associate to ensure that any subcontractors it may engage on its behalf that will have access to PHI must agree to the same restrictions and conditions that apply to the Business Associate with respect to its handling of PHI; and

- BAAs must provide for the Covered Entity's right of termination if the Business Associate violates a material term of the BAA. BAAs between a Business Associate and its subcontractor must have an equivalent provision.

In addition to the terms required by HHS, we strongly recommend that other terms be integrated into any high-risk (significant PHI being transmitted, received, processed, stored, etc.) BAA by the parties. For example, a Business Associate should indemnify a Covered Entity for damages accruing by reason of breaches of the HIPAA Final Rule by the Business Associate, and such indemnification obligations could be carved out of the limitation of liability. A Covered Entity can similarly indemnify a Business Associate for damages caused by the Covered Entity's HIPAA breaches. There are several other provisions advisable to include.

Although HHS OCR states that it is possible for Covered Entities and Business Associates, and Business Associates and their subcontractors, to enter into stand-alone BAA supplements separate and apart from the substantive agreements (the BAAs) governing their business relationship, better practice in almost all high-risk cases is to incorporate necessary BAA provisions and those advisable above and beyond the minimum, into a short addendum document to the underlying BAA, which modifies and incorporates it. In some low-risk cases (small amounts of PHI being transmitted pursuant to the BAA), a "plain vanilla" stand-alone version of the HIPAA Final Rule Sample Terms simply making reference to the underlying BAA may be sufficient. In a third, small number of cases, in which the BAA is expiring, or is up for renewal, or was incompetently drafted

originally, it may be prudent and cost-effective to prepare a full amendment and restatement of the BAA, incorporating the HIPAA Final Rule Sample Terms and others into the main body of the BAA. This is because of several factors:

- BAA terms based on the HIPAA Final Rule Sample Terms contained in a separate stand-alone agreement (as opposed to an incorporated addendum) from the substantive agreement invite ambiguity as to which transactions under the substantive agreement are covered. Although careful drafting can minimize this effect, the risk of partially overlapping and inconsistent terms, definitions and gaps between the coverage in provisions are minimized in an integrated agreement incorporating both the substantive business terms and BAA terms (particularly because simple use of the HIPAA Final Rule Sample Terms is not going to result in that kind of careful drafting);

- Business Associates may be unwilling to sign stand-alone BAA supplements, under which they are not being paid, but will more readily sign BAA addendums relating to the underlying BAA and incorporating the BAA terms;

- The remedies, rights of termination, confidentiality, warranty, indemnification and limitation of liability, among others, contained in the substantive BAA, in which the Covered Entity is probably paying the Business Associate for its services, can more readily be negotiated than is the case in a stand-alone BAA supplement, in which the Business Associate is not being paid by the Covered Entity, and the Business Associate is not offering services to the Covered Entity; and

- BAA terms incorporated by reference into the substantive agreement will be more customized and optimized towards protecting PHI in that relationship's context, as can be seen in the resume of required BAA terms, below, than would be the case in a stand-alone BAA supplement containing general terms and not optimized for any specific Business Associate relationship - for example, the case of a BAA requiring the Business Associate to carry out any of the Covered Entity's obligations under the HIPAA Privacy Rule.

V. Conclusion

The foregoing principles, optimized and customized for the individual business relationship between a Covered Entity and its Business Associate, or between a Business Associate and its subcontractor, and complied with during the BAA's term, should provide protection against the enhanced civil and criminal penalties now applicable to mishandling of PHI under the HIPAA Final Rule. Covered Entities should audit and review their PHI-sensitive contracts pre-dating January 25, 2013 (treating all contracts under which access to PHI is given to a Business Associate as a material contract) and plan an amendment or modification of the agreement incorporating and integrating BAA terms, as so customized and optimized for the business relationship, prior to the September 22, 2014 deadline. In addition, all post-January 25, 2013 BAAs and all new BAAs must be HIPAA Final Rule – compliant *now*. Business Associates need to realize their new status as such under the HIPAA Final Rule and take a proactive stance towards BAA and overall compliance as befits their new, direct and primary liability for the same civil and criminal penalties. An on-going compliance program and a protocol

for new BAAs that may be entered into should also be adopted, recognizing that all new BAAs must be immediately HIPAA Final Rule - compliant, and that the September 22, 2014 deadline applies only to BAAs entered into before January 25, 2013. A schedule of the HIPAA/HITECH civil fines now applicable to Covered Entities and Business Associates follows as Appendix A.

Owen Kurtin

Appendix A: Civil Fine Schedule

Violation Category	Each Violation	Aggregate Maximum of Violations of same provision in a Calendar Year
A. Covered Entity did Not Know act was a HIPAA violation (and by exercising reasonable diligence would not have known)	$100 - $50,000	$1,500,000
B. HIPAA violation had a Reasonable Cause and was not due to Willful Neglect	$1,000 - $50,000	$1,500,000
C. (i) HIPAA Violation was due to Willful Neglect but Violation was Corrected Timely	$10,000 -$50,000	$1,500,000
C. (ii) HIPAA Violation was due to Willful Neglect and was Not Corrected	$50,000 +	$1,500,000