HIPAA BUSINESS ASSOCIATE AGREEMENT BEST PRACTICES

January 2018

I. Executive Summary.

The Health Insurance Portability and Accountability Act ("HIPAA") is a federal law passed by Congress in part to protect medical patient data privacy from misuse or disclosure by healthcare providers and companies providing services to the healthcare industry. The law, along with regulations promulgated by the U.S. Department of Health and Human Services (HHS) (the collected regulations, as finalized in 2013, are known as the "HIPAA Omnibus Rule"), provides for *extremely high civil fines and criminal penalties for even unintentional breaches of its provisions, and those fines have been steadily increasing in both frequency and amount – up to several million dollars per incident.* Because prior versions of HIPAA did not have such severe penalties and did not make service providers directly liable for them, many in the healthcare industry and its service providers developed a culture of casual compliance with the law and rules. In the meantime, the HHS Office of Civil Rights (OCR) is imposing multi-million dollar penalties for unintentional breaches arguably not even involving negligence.

The relationship between healthcare providers, called "Covered Entities" by HIPAA, and their service providers, called "Business Associates," must be governed by a written contract with required provisions called a "Business Associate Agreement." The Business Associate Agreement has become the critical document governing the relationship between Covered Entities and Business Associates, and allocating their rights, responsibilities and obligations. Because of the previous low regulatory risk of the Covered Entity – Business Associate relationship, they often treated Business Associate Agreements as a relatively *pro forma* document. Many Business Associates did not know that they *were* Business Associates in that relationship, and subject to HIPAA requirements. That has all changed in light of the new civil and criminal penalties, and the Business Associate Agreement is now a bilateral contract allocating potentially millions of dollars in civil fines, criminal liability, and even private class action lawsuits that must be carefully negotiated, drafted and customized for the relationship and the services involved. This advisory will discuss critical issues to consider for Business Associate Agreements when entering into a HIPAA-controlled Covered Entity – Business Associate relationship and describe Kurtin PLLC's compliance solution.

II. Who is Affected?

The HIPAA Omnibus Rule, published by HHS pursuant to the "HITECH" (Health Information Technology for Economic and Clinical Health) Act and the Genetic Information Nondiscrimination Act, makes all HIPAA Covered Entities *and their Business Associates* (both defined below) *primarily and directly liable* for compliance with the law's patient data privacy requirements. For purposes of the HIPAA Omnibus Rule, "Covered Entities" include:

- Health care providers (doctors, clinics, hospitals, medical centers, psychologists, dentists, chiropractors, nursing homes and pharmacies, when transmitting patient protected health information, or "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). For example, cloud data storage providers, billing services, data processing outsourcing services, medical device manufacturers and other Covered Entities may all be Business Associates in a given Covered Entity relationship.

III. The HIPAA Omnibus Rule and Enforcement: the Enhanced Civil Fine and Criminal Penalty Regime.

The HIPAA Omnibus Rule changed 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.* 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. A full schedule of the civil fines is appended to the end of this advisory as

Appendix A. *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.* A full schedule of the criminal penalties is appended as Appendix B.

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 developed a culture of not taking them seriously. Additionally, because Business Associates were not directly and primarily liable under HIPAA before the HIPAA Omnibus Rule, many service providers to Covered Entities do not even realize that they are HIPAA - regulated Business Associates.

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 2016 alone, there were 13 OCR HIPAA fines imposed or settlements agreed to (so-called "resolution agreements"), totaling just over $23.5 million, and which focused heavily on breaches of the Business Associate Agreement requirements; in 2017 total fines and settlements totaled over $19 million. Among settlements imposed between 2015 and 2017 were:

- $5.55 million against Advocate Health Care of Illinois for failure to maintain compliant Business Associate Agreements with Business Associates, as required by the HIPAA Security and Privacy Rules and failure to conduct an accurate and thorough risk analysis, as required by the HIPAA Security Rule (this was the largest single HIPAA penalty yet imposed);

- $5.5 million against Memorial Healthcare Systems for failure to maintain audit controls and other violations, and for permitting disclosure of patient PHI;

- $3.5 million against Triple-S Management Corporation (formerly known as American Health Medicare Inc.) for multiple violations, including *"Impermissible disclosure of its beneficiaries' PHI to an outside vendor with which it did not have an appropriate business associate agreement;"*

- $2.5 million against CardioNet for multiple areas of noncompliance and for disclosure of PHI;

- $2.4 million against Memorial Hermann Health System for disclosures of patient PHI;

- $2.3 million against 21st Century Oncology for multiple HIPAA violations;

- $1.55 million against North Memorial Healthcare for failure to identify a Business Associate and put a Business Associate Agreement in place, allowing the Business Associate to gain unauthorized access to PHI;

- $650,000 against Catholic Health Care Services of the Archdiocese of Philadelphia, a Business Associate, for failing to maintain Business Associate Agreements with Covered Entities. This resolution, although not the largest, is noteworthy for being *the first ever levied directly against a Business Associate itself, establishing that OCR intends for the HIPAA Omnibus Rule's imposition of primary and direct liability against Business Associates to have teeth (as do the currently pending Phase II OCR audits of Business Associates);*

- $2.7 million against Oregon Health & Science University, in part for storing PHI on non-Business Associate Google's cloud storage service;

- $750,000 against Raleigh Orthopaedic Health Clinic, for giving access to PHI to a vendor without a Business Associate Agreement in place. "HIPAA's obligation on covered entities to obtain business associate agreements is more than a mere check-the-box paperwork exercise," OCR Director Jocelyn Samuels said. "It is critical for entities to know to whom they are handing PHI and to obtain assurances that the information will be protected.; and

- $400,000 against Care New England Health System for failure to maintain updated Business Associate Agreements compliant with the 2013 HIPAA Omnibus Rule.

In all, HHS has collected over $67 million in HIPAA fines and settlements, over $42 million of that in 2016 and 2017 alone. The frequency and severity of OCR resolution settlements is rapidly increasing, and the Business Associate Agreement issue is clearly front and center on OCR's radar screen. None of the illustrated examples involved any venal or other bad motive; the worst that can be said was that the behavior that led to the HIPAA data breach for which the fine was imposed was reckless or negligent – by HHS's standards. If any of the above scenarios sound like something that could happen in the reader's organization, this issue is critical.

IV. What Constitutes a HIPAA Breach?

The HIPAA Omnibus Rule, as stated, makes all Covered Entities and 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 Omnibus 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 Omnibus 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 HIPAA Security Rule; and
- Contractual liability under the Business Associate Agreement.

V. Business Associate Agreements.

The mandatory framework for the relationship between Covered Entities and Business Associates are the written service agreements or contracts between them, called "Business Associate Agreements," which are subject to HIPAA regulatory requirements. The recent multiple HHS OCR resolution settlements confirm that *it is a facial violation of HIPAA for a Covered Entity to transmit, and for a Business Associate to receive, PHI without a written, compliant Business Associate Agreement in place. See 45 C.F.R. §164.314(a)(2)(1). In other words, if there is no written, compliant Business Associate Agreement in place, the Covered Entity had no right to transmit, and the Business Associate had no right to receive, the PHI in the first place.*

As a practical matter, all agreements by Covered Entities with third parties who electronically receive, process, store, maintain or retransmit a Covered Entity's PHI are Business Associate Agreements, and must be reviewed and HIPAA-required Business Associate Agreement terms incorporated, customized and optimized for the particular business relationship involved; and the contractual counter-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 Business Associate Agreement provisions are actually complied with throughout the life of the agreement.

Many Covered Entities and Business Associates are under the impression that the dozen or so of HHS OCR - suggested Business Associate Agreement terms that are floating around the Internet on various forms are Business Associate Agreements themselves. *This is specifically not true, and HHS OCR warns against this assumption on its Business Associate Agreement webpage.* In fact, Business Associate Agreements are really the underlying service agreements *of whatever type* between Covered Entities and Business Associates, or between Business Associates and their subcontractors, pursuant to which patient PHI is electronically transmitted, received, stored, maintained or processed. *A Business Associate Agreement may be a software license agreement, a data storage agreement, an outsourcing 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. Many large Covered Entities and Business Associates have tens of thousands of such contracts in place – or they should. The short-form sets of terms and conditions found on-line are *not* Business Associate Agreements, they are only versions of 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 Business Associate Agreements of whatever type, between whatever type of Covered Entity and Business Associate, or Business Associate and subcontractor. Call them the "HIPAA Omnibus Rule Sample Terms."

HHS OCR *did not* intend the HIPAA Omnibus Rule Sample Terms to become a short-form, catchall compliance solution. The HHS OCR website states of the HIPAA Omnibus 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, and does not replace consultation with a lawyer or negotiations between the parties to the contract." See:* https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html (January 25, 2013).

Subject to the foregoing, the following minimum standards for Business Associate Agreements apply:

- Business Associate Agreements must be written, executed agreements between Covered Entities and Business Associates and between Business Associates and their subcontractors;

- Business Associate Agreements must establish the permitted and required uses and disclosures of PHI by the Business Associate;

- Business Associate Agreements must provide that the Business Associate will not use or further disclose the information other than as required by the Business Associate Agreement or by other applicable law;

- Business Associate Agreements 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;

- Business Associate Agreements must require the Business Associate to report to the Covered Entity any

use or disclosure of the PHI not provided for in the Business Associate Agreement, including incidents that constitute breaches of unsecured PHI;

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

- If the Business Associate Agreement 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;

- Business Associate Agreements 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;

- Business Associate Agreements must provide that at the termination of the Business Associate Agreement, 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;

- Business Associate Agreements 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

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

VI. Kurtin PLLC's Compliance Solution

As HHS OCR ramps up its Phase II audits of both Covered Entities and Business Associates, and as multimillion dollar fines and resolution agreements multiply, it is important and urgent to realize that the HIPAA Omnibus Rule Sample Terms are a *minimum and non-specific* HHS OCR requirement for each contract constituting a Business Associate Agreement, 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 contractual relationship. It is important to remember that every Business Associate Agreement is a bilateral contract providing for services rendered by Business Associate to Covered Entity, and allocating potentially millions of dollars in rights, obligations and liabilities.

For example, in any high-risk Business Associate Agreement (large amounts of PHI are being electronically transmitted pursuant to its terms), the required HIPAA Omnibus Rule provisions customized for the services and parties involved should be bolstered by terms clarifying and specifying each party's duties, 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), termination rights, remedies upon termination, choice of governing law, choice of forum for dispute resolution, confidentiality and others. Terms should also be added clarifying rights and responsibilities in any pre-existing contract that had since been found to be ambiguous, or a source of contention or dissatisfaction between the parties.

Our approach to HIPAA Business Associate Agreement Best Practices involves efficient drafting – or, when a contract already exists - review and triage, of Covered Entity - Business Associate bilateral contracts of whatever type and adaptation of both HIPAA–required terms, and terms appropriate for the particular business relationship to produce a contract that is not only a HIPAA-compliant Business Associate Agreement, but one that reflects an appropriate allocation of rights, obligations and liabilities of the respective parties, and which protects the party proposing the agreement from unintended liabilities. This can be achieved most efficiently and cost-effectively, depending on circumstance, by (i) a stand-alone Business Associate Agreement, (ii) a Business Associate Agreement addendum to an existing contract focused on HIPAA compliance (and which is structured so as not to inadvertently conflict, and perhaps nullify, the existing contract's terms), or (iii) an amended and restated Business Associate Agreement. Following review, the recommendation of which way to proceed is made, and when agreed to, swiftly implemented according to a standard flat-fee schedule that includes discounts for larger volumes of contracts. Further information is available at www.kurtinlaw.com, or by e-mail at info@kurtinlaw.com.

Owen D. 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

Appendix B
Criminal Penalties

Violation Category	Each Violation
A. Unknowingly or with reasonable cause	Up to one year
B. Under false pretenses	Up to five years
C. For personal gain or malicious reasons	Up to ten years

Kurtin PLLC is a New York City-based law firm focused on corporate, commercial and regulatory representation in the Biotechnology & Life Sciences, Communications & Media, Information Technologies and Satellites & Space sectors. For further information, please see our website at www.kurtinlaw.com and contact info@kurtinlaw.com.