THOMAS D. BIXBY
LAW OFFICE LLC

LEGAL ADVICE FOR HEALTH PLANS

BUSINESS ASSOCIATE AGREEMENT CHECKLIST

INSTRUCTIONS

This checklist is designed as an aid in determining whether a health plan's ("Health Plan's) business associate agreement contains the provisions required by the HIPAA Breach Notification, Security, and Privacy Rules (45 C.F.R. Part 164) ("HIPAA").

The checklist should not be construed as legal advice or a legal opinion with respect to any specific agreement or specific set of facts and circumstances. The checklist is intended solely for general purposes. You should consult an attorney concerning any specific agreement or legal questions you may have.

REQUIRED PROVISIONS

□ The Agreement must establish Business Associate's permitted and required uses for and disclosures of protected health information (PHI).

□ The Agreement may not, however, permit Business Associate to use or disclose PHI in a manner that would violate the Privacy Rule if Health Plan made the use or disclosure, except Business Associate may be permitted to:

- ✓ Use or disclose PHI for Business Associate's proper management and administration (in limited circumstances).
- ✓ Aggregate the data of several covered entities to perform health care operations on each covered entity's behalf.

□ The Agreement must prohibit the use or disclosure of PHI, except as the Agreement permits or as required by law.

□ SAFEGUARDS:

- ✓ PRIVACY: Business Associate must use reasonable and appropriate safeguards to protect the privacy of PHI.
- ✓ SECURITY: Business Associate must comply with the Security Rule (45 C.F.R. Part 164, Subpart C).

□ INCIDENT REPORTING:

- ✓ BREACH NOTICE: Business Associate must report to Health Plan any "breach" for which notice is required under the Breach Notification Rule (45 C.F.R. Part 164, Subpart D).
- ✓ PRIVACY: Business Associate must report to Health Plan any non-permitted use or disclosure of PHI (even if the incident is not a "breach" under Breach Notification Rule).
- ✓ SECURITY: Business Associate must report any Security Incident.

□ Business Associate must provide to Health Plan PHI in a "designated record set" so Health Plan can comply with an individual's access rights under 45 C.F.R. § 164.524.

□ Business Associate must permit Health Plan to amend records in a designated record set as required by 45 C.F.R. § 164.526.

□ Business Associate must track disclosures for which accounting is required and provide a list of such disclosures to Health Plan as necessary for Health Plan to comply with an individual's disclosure accounting rights under 45 C.F.R. § 164.528.

❒ If Business Associate discloses PHI to a subcontractor, Business Associate must engage the subcontractor in a written agreement that incorporates the same restrictions and conditions concerning PHI that apply to Business Associate.

❒ Business Associate must permit Covered Entity to terminate the Agreement in case of a material violation of the Agreement.

❒ Business Associate must make its internal practices, books, and records relating to the use and disclosure of PHI available to HHS for purposes of determining Health Plan's compliance with the Privacy Rule.

❒ If Business Associate is to carry out an obligation imposed by HIPAA on Health Plan (*i.e.*, provide privacy practices notices or comply with access requests), the Agreement must require Business Associate to perform the function in compliance with the Health Plan's obligations under HIPAA.

❒ Upon termination of the Agreement, Business Associate must return or destroy the PHI it received under the Agreement, if feasible. Business Associate must continue to safeguard any PHI it cannot feasibly return or destroy and use or disclose it only for the reasons that make return or destruction infeasible.

OTHER TERMS COVERED ENTITY MAY WISH TO CONSIDER

HEALTH PLAN MAY WISH TO IMPOSE ON BUSINESS ASSOCIATE AN OBLIGATION TO:

❒ Abide by any restriction request or confidential communication request to which Health Plan agrees. *See* 45 C.F.R. §§ l64.522(a), (b).

❒ Use, disclose, and request the minimum PHI necessary to accomplish the intended purpose of the use, disclosure, or request. *See* 45 C.F.R. §§ 164.502(b), 514(d).

❒ Mitigate harmful effects of impermissible uses or disclosures of PHI. *See* 45 C.F.R. § 164.530(f).

❒ Make Business Associate's internal practices, books, and records relating to the use and disclosure of PHI available to Health Plan (so Health Plan can be prepared for response to HHS investigation). *See* 45 C.F.R. § 164.504(e)(2)(ii)(H).

❒ Prohibit (i) the use of "genetic information" for "underwriting"; (ii) the sale of PHI; and (iii) the use or disclosure of PHI for "marketing." *See* 45 C.F.R. §§ 164.501 ("marketing"); 164.502(a)(5)(i); (ii).

❒ Limit reporting requirements for "unsuccessful" Security Incidents, such as pings on firewall, port scans, unsuccessful log-on attempts, etc.

❒ Require Business Associate to indemnify Health Plan for violation of terms of agreement and/or any "breach" for which notice is required.

❒ Include provisions to address records containing Substance Use Disorder Patient Identifying Information pursuant to 42 C.F.R. Part 2, if applicable.

❒ Conduct transactions in standard format under any circumstances in which Health Plan would be required to do so. *See* 45 C.F.R. § 162.923(c).

❒ Cooperate with Health Plan to certify compliance with Transactions Rule and CORE Operating Rules. *See* Social Security Act § 1173(h)(1)(A).

❒ Encrypt PHI in various circumstances. *See* Breach Notification Rule (45 C.F.R. Part 164, Subpart D).

❒ Use and disclose PHI in compliance with Health Plan's privacy practices notice. *See* 45 C.F.R. § 164.502(i).