Altomare
FINANCIAL GROUP, INC.

1680 Route 23 North ● Suite 310 ● Wayne, NJ 07470 **Tel:** 973.812.7788 **Fax:** 973.812.0719

BUSINESS ASSOCIATE AGREEMENT

HIPAA "Omnibus" Final Rule Update

This Agreement is made effective _____ by and between **ALTOMARE FINANCIAL GROUP, INC.**, hereinafter referred to as "Covered Entity", and **BUSINESS ASSOCIATE NAME**, hereinafter referred to as "Business Associate", (individually, a "Party" and collectively, the "Parties").

WITNESSETH:

WHEREAS, Sections 261 through 264 of the federal Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, known as "the Administrative Simplification provisions," direct the Department of Health and Human Services to develop standards to protect the security, confidentiality and integrity of health information; and

WHEREAS, pursuant to the Administrative Simplification provisions, the Secretary of Health and Human Services has issued regulations modifying 45 CFR Parts 160 and 164 (the "HIPAA Privacy Rule" and the "HIPAA Security Rule"); and

WHEREAS, Title XIII of the American Recovery and Reinvestment Act, known as "the HITECH Act" has amended HIPAA and the HIPAA regulations, including HIPAA's Administrative Simplification provisions; and

WHEREAS, amendments to the HIPAA Regulations contained in the HIPAA Omnibus Final Rule became effective on March 26, 2013, and amended HIPAA's Privacy, Security, Breach Notification and Enforcement Rules; and

WHEREAS, The requirements of the HIPAA Administrative Simplification Regulations (including the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules) implement sections 1171-1180 of the Social Security Act (the Act), sections 262 and 264 of Public Law 104-191, section 105 of 492 Public Law 110-233, sections 13400-13424 of Public Law 111-5, and section 1104 of Public Law 111-148.

WHEREAS, the Parties wish to enter into or have entered into an arrangement whereby Business Associate will provide certain services to Covered Entity, and, pursuant to such arrangement, Business Associate may be considered a "Business Associate" of Covered Entity as defined in the HIPAA Privacy Rule; and

WHEREAS, Business Associate may have access to Protected Health Information (as defined below) in fulfilling its responsibilities under such arrangement;

THEREFORE, in consideration of the Parties' continuing obligations under the HIPAA Privacy Rule and Security Rule, and other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the Parties agree to the provisions of this Agreement in order to address the requirements of the HIPAA Privacy Rule and Security Rule and to protect the interests of both Parties.

I. DEFINITIONS

Except as otherwise defined herein, all terms in this Agreement shall have the definitions set forth in the current HIPAA Rules. In the event of an inconsistency between the provisions of this Agreement and mandatory provisions of the HIPAA Rules, as amended, the HIPAA Rules shall control. Where provisions of this Agreement are different than those mandated in the HIPAA Rules, but are nonetheless permitted by the HIPAA Rules, the provisions of this Agreement shall control.

Protected Health Information -- The term "Protected Health Information" (abbreviated as "PHI") means individually identifiable health information including, without limitation, all information, data, documentation, and materials, including without limitation, demographic, medical and financial information, that relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Covered Entity – The term "Covered Entity" (abbreviated as "CE") means 1.) a health plan; 2.) a health care clearinghouse; 3.) a health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

Business Associate – The term "Business Associate" (abbreviated as ("BA") means, with respect to a Covered Entity, a person who: 1.) On behalf of such Covered Entity or of an organized health care arrangement (as defined in this section) in which the Covered Entity participates, but other than in the capacity of a member of the workforce of such Covered Entity or arrangement, creates, receives, maintains, or transmits protected health information for a function or activity regulated by this subchapter, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 CFR 3.20, billing, benefit management, practice management, and

repricing; or, 2.) Provides, other than in the capacity of a member of the workforce of such Covered Entity, legal, actuarial, accounting, consulting, data aggregation (as defined in § 164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such Covered Entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of protected health information from such Covered Entity or arrangement, or from another Business Associate of such Covered Entity or arrangement, to the person.

Business Associates, under the 2013 HIPAA Final Rule amendments, include the following:

- ❑ Subcontractors.
- ❑ Patient safety organizations.
- ❑ HIOs - Health Information Organizations, including Health Information Exchanges (HIEs) and regional Health Information Organizations.
- ❑ E-Prescribing gateways.
- ❑ PHRs - Personal Health Record vendors that provide services on behalf of a covered entity. PHR vendors that do not offer PHRs on behalf of CEs are not BAs.
- ❑ Other firms or persons who "facilitate data transmission" that requires routine access to PHI.

HIPAA Rules – The term "HIPAA Rules" means the HIPAA Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

Business Associate acknowledges and agrees that all Protected Health Information that is created or received by Covered Entity and disclosed or made available in any form, including paper record, oral communication, audio recording, and electronic media by Covered Entity or its operating units to Business Associate or is created or received by Business Associate on Covered Entity's behalf shall be subject to this Agreement.

II. CONFIDENTIALITY REQUIREMENTS

(A) Business Associate agrees:

(i) to use or disclose any Protected Health Information solely: (1) for meeting its obligations as set forth in any agreements between the Parties evidencing their business relationship, or (2) as required by applicable law, rule or regulation, or by accrediting or credentialing organization to whom Covered Entity is required to disclose such information or as otherwise permitted under this Agreement, or the HIPAA Privacy Rule or Security Rule;

(ii) at termination of this Agreement, or any similar documentation of the business relationship of the Parties, or upon request of Covered Entity, whichever occurs first, if feasible, Business Associate will return or destroy all Protected Health Information received from or created or received by Business Associate on behalf of Covered Entity that Business Associate still maintains in any form and retain no copies of such information, or if such return or destruction is not feasible, Business Associate will extend the protections of this Agreement to the information in perpetuity and limit further uses and disclosures to those purposes that make the return or destruction of the information not feasible; and

(iii) to ensure that its agents, including a subcontractor, to whom it provides Protected Health Information received from or created by Business Associate on behalf of Covered Entity, agrees to the same restrictions and conditions that apply to Business Associate with respect to such information. In addition, Business Associate agrees to take reasonable steps to ensure that its employees' actions or omissions do not cause Business Associate to breach the terms of this Agreement or the mandatory requirements of the HIPAA Privacy Rule and Security Rule that may apply to Business Associate.

(B) Notwithstanding the prohibitions set forth in this Agreement, Business Associate may use and disclose Protected Health Information as follows:

(i) if necessary, for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate, provided that as to any such disclosure, the following requirements are met:

(a) the disclosure is required by law, not merely permitted by law; or

(b) Business Associate obtains reasonable written assurances from the person or party to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person or party, and the person or party notifies Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached;

(ii) for data aggregation services, if to be provided by Business Associate for the health care operations of Covered Entity pursuant to any agreements between the Parties evidencing their business relationship. For purposes of this Agreement, data aggregation services means the combining of Protected Health Information by Business Associate with the Protected Health Information received by Business Associate in its capacity as a business associate of another covered entity, to permit data analyses that relate to the health care operations of the respective covered entities.

(c) Business Associate will implement appropriate safeguards to prevent use or disclosure of Protected Health Information other than as permitted in this Agreement. The Secretary of Health and Human Services shall have the right to audit Business Associate's records and practices related to uses and disclosures of Protected Health Information to ensure Covered Entity's compliance with the terms of the HIPAA Privacy Rule and Security Rule. Business Associate shall timely report to Covered Entity any use or disclosure of Protected Health Information which is not in compliance with the terms of this Agreement of which it becomes aware.

III. OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE

(a) Business Associate agrees that it is required under the amended HIPAA regulations to comply with, and shall comply with, the HIPAA Security Rule, including the Security Rule's Administrative, Physical, and Technical safeguard requirements.
(b) Business Associate agrees that it is required under the amended HIPAA regulations to comply with, and shall comply with, the use and disclosure provisions of the HIPAA Privacy Rule.
(c) Business Associate agrees to not use or disclose Protected Health Information other than as permitted or required by the Agreement or as required by law.
(d) Business Associate agrees that it may not use or disclose Protected Health Information in a manner that would violate Subpart E of 45 CFR Part 164 if done by Covered Entity.
(e) Business Associate agrees to use appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information, to prevent use or disclosure of Protected Health Information other than as provided for by this Agreement.
(f) Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business Associate in violation of the requirements of this Agreement.
(g) Breach Disclosures to Covered Entity: Business Associate agrees to immediately report to Covered Entity any use or disclosure of Protected Health Information not provided for by this Agreement of which it becomes aware; and any security incident of which it becomes aware. Further, Business Associate agrees to notify the Covered Entity of any individual whose Protected Health Information has been inappropriately or unlawfully released, accessed, or obtained. Business Associate agrees that such notification will meet the requirements of 45 CFR 164.410 of the amended HIPAA regulations. Specifically, the following shall apply:
    i. A breach is considered discovered on the first day the Business Associate knows or should have known about it.
    ii. In no case shall the Business Associate notify the Covered Entity of any breach later than 24 hours.
    iii. Business Associate shall notify the Covered Entity of any and all breaches of Protected Health Information, and provide detailed information to the Covered Entity about the breach, along with the names and contact information of all individuals whose Protected Health Information was involved.
    iv. For breaches determined to be caused by the Business Associate, where such breaches require notifications to patients or consumers, the cost of such breach notifications shall be borne by the Business Associate.

(h) Business Associate agrees, in accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, to ensure that any subcontractors that create, receive, maintain, or transmit Protected Health Information on behalf of the Business Associate agree to the same restrictions, conditions, and requirements that apply to the Business Associate with respect to such information;
(i) Business Associate agrees to apply HIPAA's Minimum Necessary Standard to all uses, disclosures, and requests for Protected Health Information, and to make reasonable efforts to limit the Protected Health Information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.
(j) Business Associate agrees to provide access, at the request of Covered Entity, in a reasonable time and manner to Protected Health Information in a Designated Record Set, to Covered Entity or, as directed by Covered Entity, to an Individual in order to meet the requirements of 45 CFR § 164.524.
(k) Business Associate agrees to make any amendment(s) to Protected Health Information in a Designated Record Set that the Covered Entity directs or agrees to pursuant to 45 CFR § 164.526 at the request of Covered Entity or an Individual in a reasonable time and manner.
(l) Business Associate agrees to make internal practices, books, and records, including policies and procedures and Protected Health Information, relating to the use and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of, Covered Entity available to the Covered Entity or to the Secretary, in reasonable time and manner or designated by the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the HIPAA Privacy Rule and Security Rule.
(m) Business Associate agrees to document such disclosures of Protected Health Information and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR § 164.528.
(n) Business Associate agrees to provide to Covered Entity or an Individual in a reasonable time and manner information collected in accordance with Section III (i) of this Agreement, to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR § 164.528.
(o) Business Associate agrees to comply with the requirements of the "Red Flags" Rule and implement a compliant identity theft prevention program by or before the required "Red Flags" Rule compliance date, and ongoing thereafter.
(p) Business Associate agrees to adhere to the terms and conditions that shall specifically address compliance with Horizon BCBSNJ Regulations, including Horizon BCBSNJ underwriting rules and compliance programs as well as the Sub-Producer's obligation to affirmatively cooperate with any Horizon BCBSNJ audit, investigation, or fraud related inquiries. Further, as part of its arrangement with the Business Associate, Altomare Financial Group agrees to implement adequate oversight and compliance programs to monitor its assigned Business Associate compliance with Horizon BCBSNJ Regulations, directives, rules, and all other applicable laws, regulations, and governmental directives.

IV. AVAILABILITY OF PHI

(a) Business Associate agrees to make available Protected Health Information to the extent and in the manner required by Section 164.524 of the HIPAA Privacy Rule.
(b) Business Associate agrees to make Protected Health Information available for amendment and incorporate any amendments to Protected Health Information in accordance with the requirements of Section 164.526 of the HIPAA Privacy Rule.

(c) In addition, Business Associate agrees to make Protected Health Information available for purposes of accounting of disclosures, as required by Section 164.528 of the HIPAA Privacy Rule.

V. TERMINATION

Notwithstanding anything in this Agreement to the contrary, Covered Entity shall have the right to terminate this Agreement immediately if Covered Entity determines that Business Associate has violated any material term of this Agreement. If Covered Entity reasonably believes that Business Associate will violate a material term of this Agreement and, where practicable, Covered Entity gives written notice to Business Associate of such belief within a reasonable time after forming such belief, and Business Associate fails to provide adequate written assurances to Covered Entity that it will not breach the cited term of this Agreement within a reasonable period of time given the specific circumstances, but in any event, before the threatened breach is to occur, then Covered Entity shall have the right to terminate this Agreement immediately.

Upon termination of this Agreement for any reason, Business Associate agrees to return to Covered Entity all Protected Health Information received from Covered Entity, or created, maintained, or received by Business Associate on behalf of Covered Entity, that the Business Associate still maintains in any form. Business associate shall retain no copies of the Protected Health Information in any form or medium.

VI. MISCELLANEOUS

Except as expressly stated herein or in the HIPAA Rules, the parties to this Agreement do not intend to create any rights in any third parties. The obligations of Business Associate under this Section shall survive the expiration, termination, or cancellation of this Agreement, and/or the business relationship of the parties, and shall continue to bind Business Associate, its agents, employees, contractors, successors, and assigns as set forth herein.

This Agreement may be amended or modified only in a writing signed by the Parties. No Party may assign its respective rights and obligations under this Agreement without the prior written consent of the other Party. None of the provisions of this Agreement are intended to create, nor will they be deemed to create any relationship between the Parties other than that of independent parties contracting with each other solely for the purposes of effecting the provisions of this Agreement and any other agreements between the Parties evidencing their business relationship. This Agreement shall be governed by the laws of the State of New Jersey. No change, waiver or discharge of any liability or obligation hereunder on any one or more occasions shall be deemed a waiver of performance of any continuing or other obligation, or shall prohibit enforcement of any obligation, on any other occasion. The parties agree that, in the event that any documentation of the arrangement pursuant to which Business Associate provides services to Covered Entity contains provisions relating to the use or disclosure of Protected Health Information which are more restrictive than the provisions of this Agreement, the provisions of the more restrictive documentation will control. The provisions of this Agreement are intended to establish the minimum requirements regarding Business Associate’s use and disclosure of Protected Health Information.

In the event that any provision of this Agreement is held by a court of competent jurisdiction to be invalid or unenforceable, the remainder of the provisions of this Agreement will remain in full force and effect. In addition, in the event a party believes in good faith that any provision of this Agreement fails to comply with the then-current requirements of the HIPAA Privacy Rule or Security Rule, such party shall notify the other party in writing, For a period of up to thirty days, the parties shall address in good faith such concern and amend the terms of this Agreement, if necessary to bring it into compliance. If, after such thirty-day period, the Agreement fails to comply with the requirements of the HIPAA Privacy Rule and Security Rule, then either party has the right to terminate upon written notice to the other party.

IN WITNESS WHEREOF, the Parties have executed this Agreement as of the day and year written above.

COVERED ENTITY:	**BUSINESS ASSOCIATE:**
By:_____	By:_____
Title:_____	Title:_____
Date:_____	Date:_____

Business Associates - Guidance from The HIPAA Group

Business Associates (BAs)

The Omnibus Rule expands the definition of a “business associate” to generally include all those entities that create, receive, maintain, or transmit PHI on behalf of a CE.

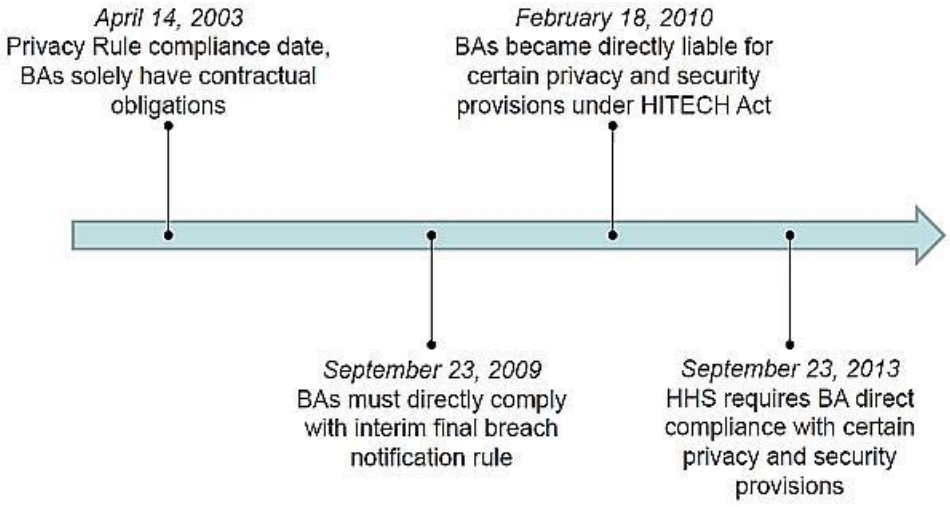
BAs under the Final Rule provide certain identified services *involving PHI* (rather than just IIHI).

The Final Rule also specifically identifies the following types of entities as business associates:

1. Subcontractors.
2. Patient safety organizations.
3. HIOs -- Health Information Organizations (and similar organizations). HHS declined to specifically define HIOs in the Omnibus Rule, but chose the term "HIO" because it includes both Health Information Exchanges (HIEs) and regional health information organizations.
4. E-Prescribing gateways.
5. PHRs -- Personal Health Record vendors that provide services on behalf of a covered entity. PHR vendors that *do not* offer PHRs on behalf of CEs are *not* BAs.
6. Other firms or persons who “facilitate data transmission" that requires routine access to PHI.

BAs (including their subcontractors) now are subject to civil money penalties and other enforcement actions for noncompliance. Like CEs, BAs may also be liable for violations by their agents.

Timeline of Business Associate Obligations under HIPAA



Minimum Necessary Standard Now Applies Directly to BAs

The Omnibus Rule applies the "minimum necessary" standard directly to BAs and their subcontractors. When using, disclosing or requesting PHI, all these entities must "make reasonable efforts to limit [the PHI] to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request."

BA Subcontractors

Subcontractors of business associates are now the same category as business associates, in the compliance sense.

Subcontractor + PHI = Business Associate!

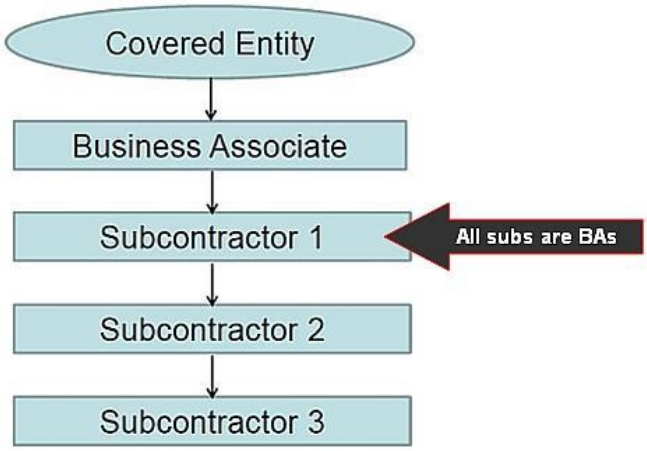
The Omnibus Rule pulls subcontractors into the definition of business associates. Under the Omnibus Rule, a subcontractor is defined as a person or entity to whom a BA delegates a function, activity, or service, and who is *not* a member of the BA's workforce.

This means that a subcontractor of a BA that creates, receives, maintains, or transmits PHI on behalf of the first or primary BA, is now itself a BA and subject to the HIPAA provisions applicable to BAs.

The Omnibus Rule did not change the definition of business associate, but instead simply adds subcontractors to the list of entities that are included as BAs.

Therefore, the business associate who contracts with the covered entity, the business associate's subcontractor, and any subcontractor of a subcontractor—all the way down the chain – are business associates to the extent they create, receive, maintain, or transmit PHI.

The CE-BA Chain



The Omnibus Rule makes clear that a covered entity is not required to enter into a contract or other arrangement with a BA that is a subcontractor—that is the responsibility of the primary or first tier BA.

Q -- When is a Subcontractor *not* a BA?

A -- When a subcontractor is assisting with a BA's *own* management, administration, or legal responsibilities. The BA still must obtain reasonable assurances of confidentiality from the subcontractor, plus assurance of notification from the subcontractor in case of breach, loss, or compromise of data.

Who is *not* a BA?

- ❑ Health Care Providers (for treatment purposes)
- ❑ Health Plan Sponsors (for plan sponsor activities after plan amendments and certifications)
- ❑ Government Agencies (for determining eligibility for or enrollment in a government health plan)
- ❑ Covered Entities that participate in an OHCA (for functions on behalf of the OHCA)
- ❑ External Researchers (for research activities)
- ❑ IRBs (in performing research review, approval, and continuing oversight)
- ❑ Financial institutions (for cashing checks or conducting funds transfer)
    - Subject to the Section 1179 exemption
- ❑ Onsite Contractors (when treated as workforce)
- ❑ Medical Liability Insurers (when CE purchases a health plan product or other insurance)

The Business Associate Conduit Exception

HHS reiterated that the definition of a BA does not include "conduits" who:

1. Transport PHI; and,
2. Do not access PHI other than on a random or infrequent basis to support transport or as required by law.

<u>The Conduit Exception</u>:

- ❑ Is limited to transmission services (whether digital or hard copy), including temporary storage incident to transmission
- ❑ Does not include an entity that maintains PHI on behalf of a covered entity, e.g., digital or hard copy "document storage companies"

It does not matter whether the entity maintaining the PHI actually views the PHI. And HHS did not address whether entity with only encrypted information (and without key) is a BA.

The Conduit Exception includes:

- ❑ U.S. Postal Service, FedEx, UPS, etc.
- ❑ ISPs who merely provide data transmission services

BA Direct Liability

The Omnibus Rule makes business associates directly liable for compliance with many of the same standards and implementation specifications under the security rule and applies the same penalties to business associates that apply to covered entities.

Under the privacy rule, business associates may use or disclose PHI only in accordance with their business associate contracts or as required by law. Moreover, a business associate may not use or disclose PHI in a manner prohibited by the privacy rule if done by a covered entity (unless HIPAA specifically permits such use and disclosure for business associates). A BA may only use or disclose information in the same manner as the CE. Therefore, any Privacy Rule limitations on how a CE uses or discloses PHI automatically extend to a business associate, and create direct liability for the BA.

The Final Rule adopted the proposal to apply the Minimum Necessary standard directly to BAs when using or disclosing PHI, or when requesting PHI from another CE. It is up to the discretion of the contracting parties to determine to what extent the BA Agreement will include specific Minimum Necessary provisions. HHS intends to issue further guidance on the Minimum Necessary standard with respect to BAs.

Not all of the requirements of the Privacy Rule apply to business associates.

For example, business associates do not need to provide a notice of privacy practices or designate a privacy official (unless the covered entity has chosen to delegate such a responsibility to the business associate, which then would make it a contractual requirement for which contractual liability would attach).

Furthermore, BAs must obtain "satisfactory assurances" in the form of business associate contracts from their subcontractor business associates. Finally, business associates must furnish any information that HHS requires to investigate whether the business associate is in compliance with the regulations.

BAs are Directly Liable under HIPAA for the Following:

1. Impermissible uses and disclosures;
2. Failure to provide breach notification to the CE;
3. Failure to provide access to a copy of electronic PHI to either the CE, the individual, or the individual's designee (whichever is specified in the BAA);
4. Failure to disclose PHI where required by HHS to investigate or determine the business
5. BA's general, overall compliance with HIPAA, as required;
6. Failure to provide an accounting of disclosures; and
7. Failure to comply with the applicable requirements of the Security Rule.

BA Duties under HIPAA Fall into Four General Categories....

1. **Required by HIPAA (penalties for noncompliance)**
   - ❑ Limit uses and disclosures of PHI
     i. Pursuant to HIPAA
     ii. Pursuant to BAA
   - ❑ Notify CE or upstream BA of breach of unsecured PHI.
   - ❑ Provide electronic copy of designated record set to CE, upstream BA, or individual (as set forth in BAA) to respond to request for access.
   - ❑ Disclose records (including PHI) to HHS for HHS HIPAA investigation.
   - ❑ Provide an accounting of disclosures.
   - ❑ Comply with the Security Rule
     i. General requirements
     ii. Administrative safeguards
     iii. Physical safeguards
     iv. Technical safeguards
     v. Organizational requirements
     vi. Policies and documentation

2. **Required Only by BA Agreement (Non-compliance = Breach of Contract)**
   - ❑ Safeguards for hard copy and verbal PHI
   - ❑ Report impermissible uses and disclosures that do not qualify as a breach of unsecured PHI
   - ❑ Report security incidents
   - ❑ Provide designated record set maintained in hard copy to respond to request for access
   - ❑ Ensure that appropriate agreement is in place with subcontractors (potentially punishable impermissible disclosure)
   - ❑ Make available PHI for amendments and incorporate amendments
   - ❑ Return or destroy PHI at termination

3. **Potential "Best Practices"**
   - ❑ Designate a privacy official
   - ❑ Policies and procedures governing privacy (use, disclosure, access, amendment, accounting)
   - ❑ Training on privacy
   - ❑ Sanctions policy for privacy noncompliance
   - ❑ Document retention policy for privacy
   - ❑ Encrypt all data received, used, stored or transmitted

4. **Not Required Unless Delegated (in writing, in the BAA)**
   - ❑ HIPAA-compliant Notice of Privacy Practices
   - ❑ Complaint process

BA Agreements

The Omnibus Rule includes up to a one-year extension for CEs and BAs to revise their BA Agreements, if such agreements were entered into and compliant with HIPAA as of Jan. 25, 2013 (the date of the Omnibus Rule publication in the Federal Register).

BA Agreements (BAAs) must establish uses and disclosures of PHI:

- ❑ As Required by HIPAA.
- ❑ As Permitted by HIPAA.

New and Renewed BA Agreements - Timing Options

If the parties to a BAA had a HIPAA-compliant Agreement in place before January 25, 2013, and the BAA is *not renewed* between March 26, 2013 and September 2013, then they can continue to lawfully use that BAA until September 23, 2014.

If the parties to a BAA *did not* have a HIPAA-compliant Agreement in place by January 25, 2013, then they must enter into a compliant BAA by September 23, 2013 – one year earlier than for grandfathered BAAs.

No matter what, if a BAA is renewed between September 23, 2013 and September 23, 2014, the new BAA must comply with the HIPAA Final (Omnibus) Rule.

The Omnibus Rule makes BA contracts applicable to arrangements involving a business associate and a subcontractor of that business associate in the same manner that business associate contracts apply to arrangements between a covered entity and its direct business associate. If a subcontractor creates, receives, maintains, or transmits PHI, then a BA must have a BAA with the subcontractor.

HHS emphasizes the continued need for BA contracts even though BAs now are held directly accountable for many provisions of HIPAA. HHS notes that BAA are necessary to clarify and limit permissible uses and disclosures of PHI, ensure business associates are contractually responsible for activities for which they are not directly liable under HIPAA, and clarify respective responsibilities related to patient rights, such as access to PHI.

Each agreement in the BA contract chain must be as or more stringent than the one above it regarding the uses and disclosures of PHI.

"Patterns of Activity" and HIPAA BA Compliance Status

A CE or BA is not in compliance with Business Associate obligations:

- ❑ If it knew of a pattern of activity, or practice of its business associate or subcontractor that constituted a material breach or violation of BA's or subcontractor's obligation(s);
- ❑ Unless it takes reasonable steps to cure the breach or end the violation; and if unsuccessful, terminates the arrangement, if feasible (No requirement to notify HHS).

BAs of Health Plans and Limited Data Sets

If *only* a limited data set is disclosed to a BA of a health plan for health care operations, only a data use agreement is required and a BA Agreement is *not* required.