IMPAC
AN ELEKTA COMPANY

MANAGING THE SPECTRUM OF CANCER CARE

HIPAA: Organizational Business Associates

Thomas H. Faris, Esq.
Chief Privacy Officer, VP RA/QA
IMPAC Medical Systems, Inc.

Definition: Business Associate (Reg)

A person who: (i) On behalf of such covered entity … performs, or assists in the performance of:

(A) A function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or

(B) Any other function or activity regulated by this subchapter; or

(ii) Provides… legal, actuarial, accounting, consulting, data aggregation…, 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 individually identifiable health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person. (160.103, HIPAA Privacy Rule)

"Business Associate" Relationship

- Business associate contracts … are only required for those cases in which
  - the covered entity is disclosing information to someone or some organization that will use the information on behalf of the covered entity,
  - when the other person will be creating or obtaining protected health information on behalf of the covered entity, or
  - when the business associate is providing the specified services to the covered entity and the provision of those services involves the disclosure of protected health information by the covered entity to the business associate.

(HIPAA Privacy Rule Preamble, page 64)

Security Rule

- Similar requirements for the Business Associate Agreement under the Security Rule
- Agreements are often combined or amended to include both HIPAA Privacy and Security Rule BA requirements
- When I refer to "the BAA," I refer to an agreement that satisfies both regulatory requirements
- Each rule has unique requirements for contractual provisions

Product/Service Providers as BA's

- Providing a product that is used in the clinical environment does not make a business associate
- Incidental viewing or access does not either, such as during installation or training
- However, adding more significant PHI uses or disclosures will, such as dial-in support, capturing databases for conversion or upgrade, data reporting or distribution

Myth of the HIPAA Compliant SW

- "Does your product comply with HIPAA?"
- Product compliance is in hands of the user
- Each Covered Entity has the responsibility for defining "adequate security," including the usability of information handling products
- However, the product still must include certain functionality that most customer deem necessary to support their HIPAA compliance requirements
- Certifications/Ads are meaningless, must evaluate according to the CE's requirements and policies

BAA Responsibility

- HIPAA imposes no legal responsibility upon business associates
- Perhaps, congressional oversight in scope of application
  - Only covers Providers, Health Plans, and Clearinghouses
  - Not all participants in the info handling process are discussed
- The final rules require the CE to "assign" pertinent HIPAA requirements to the BA
- Even so, the Privacy and Security rules are still not enforceable against the BA – remedy is breach of contract and the inability to continue business with CE's
- Some argument for application of criminal provisions

Business Associate "Agreements"

- Yes, responsibility of the CE's
- But BAA must comply
- Agreement should be amicably processed
- "Take-it or leave-it" agreements may not result in desired compliance practices – certainly not an agreement!

BAA – Minimal Contents

- Permitted and required uses of PHI (not beyond CE's)
- BA cannot further disclose PHI, other than as permitted by the contract or by law
- Use appropriate safeguards to ensure no further disclosure
- Report inappropriate disclosures to the CE
- Ensure that BA's subcontractors agree to same restrictions before further disclosing PHI

(164.504(e), HIPAA Privacy Rule)

BAA – Minimal Contents

- Make PHI available for patient review
- Incorporate necessary amendments into the PHI
- Provide an accounting of disclosures upon request
- Make practices and records available to the Secretary for purpose of determining CE's compliance with regs
- Return or destroy all PHI at termination. If not feasible, continue protections.
- Authorize termination upon breach of contract

(164.504(e), HIPAA Privacy Rule)

BAA – Minimal Contents

- Implement reasonable and appropriate administrative, physical, and technical safeguards to ensure the security under it's possession or control
- Ensure that BA's agents employee similar security safeguards
- Report any known security incidents to the CE
- Authorize termination of the agreement by the CE, if the CE determines the BA has materially breached the agreement

(164.314(a), HIPAA Security Rule)

Model BA Agreement (Privacy terms)

- A model agreement has been provided in the Appendix to the Preamble of the Privacy rule
- Provides an example of provisions and agreement form
- Provisions must be added to support business context and state-specific legal contract requirements
- "Bonus provision:" BA audit rights for Covered Entity

CE: No Duty to Monitor the BA

- CE must ensure that the BAA is in place prior to use, access, or disclosure of PHI
- No duty to monitor or ensure compliance
- But, must act upon notice of breach
  - Attempt to cure the breach
  - Terminate agreement if breach continues
  - If can't terminate, must report to the Secretary
- What about differences of opinion and practice
- I am certainly not going to vouch for the compliance level of BA's, though (other than IMPAC)

Some Onerous or Inappropriate BAA Terms

- Automatic or unilateral amendment
- At termination, delete all back up tapes
- Termination of "all" data
- CE audit rights
- Named insured
- Forgot to fill in the blanks / just sending a template
- Compliance with CE's systemic requirements
  - Not intended by regulations or BAA
  - May betray the BA's relationship with other CE's
  - Impracticability in actual practice

Business Associate Dangers

- BAA – is just another contract
- Data for hire
- No or poor protection systems implemented

No duty to monitor, but must watch for warning signs

Always be careful with your BA's

Before you send it…

- Even with BAA in place, still must satisfy other requirements:
  - Privilege
  - Minimum necessary
  - Secure transmission
  - Any other requirements imposed by your facility's compliance program

BA Nightmares – What we face

- Overzealous Priv/Sec Officers
  - Overly strict / unfair BAA's
  - Clearly intrusive requirements
  - Impracticable product requirements
  - Holding the BA to employee requirements
  - Burdensome data transmission requirements
- Underzealous Covered Entity Employees
  - "Here, use my password"
  - Too much information
  - "What Privacy/Security requirements?"

Privacy/Security Officer Training?

Understanding the Requirements

- Culture of misunderstanding and misinformation
- Consultants:
  - For some, HIPAA was the Y2K consultant reemployment act
  - Others can prove quite valuable
- The curse of the regulatory required manager
- Read and understand the actual requirements
  - The time investment will pay for itself in terms of understanding
  - Ultimately, the Covered Entity and/or the individual employee will be held accountable for violations of the law

Yes, we are ALL too busy!

Questions?

Thomas H. Faris, Esq.
VP RA/QA, Chief Privacy Officer
IMPAC Medical Systems, Inc.
650-623-8807, TFaris@impac.com