JCAHO
Joint Commission on Accreditation of Healthcare Organizations
Setting the Standard for Quality in Health Care

NCQA
Measuring the Quality of America's Health Care

PRIVACY CERTIFICATION
FOR BUSINESS ASSOCIATES

Functioning as a Business Associate Under HIPAA

William F. Tulloch
Director, PCBA
March 9, 2004

Background: JCAHO/NCQA and HIPAA

- JCAHO and NCQA are business associates to the organizations they accredit
- NCQA is also a researcher – using data gathered as a BA
- JCAHO and NCQA have developed the Privacy Certification for Business Associates (PCBA) program
- See BA issues from both sides

PRIVACY CERTIFICATION FOR BUSINESS ASSOCIATES

HIPAA Myths

- Business associates do not have to comply with the federal HIPAA regulations
- Business associates only have to have contracts with covered entities
- How many have heard these?
- How many believe it?

Why Comply with HIPAA?

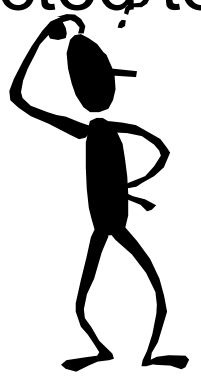
- Enforcement Issue
  - **Federal government may not enforce BA compliance, but states that adopt the federal regulations as the standard of care are likely to apply them to all organizations**
- PR Issue
  - **Public breaches of privacy or security could damage or destroy a company's reputation**
- Business Issue
  - **Covered entities need partners they can trust**
- Not to mention – it's the right thing to do!

How to Comply with HIPAA?

- According to the Privacy and Security regulations:
  - **Business associates have to provide "satisfactory assurances" that they will "appropriately safeguard" PHI (45 CFR 164.308 (b) (1) and 45 CFR 164. 502 (e) (1))**
- In both cases, specific BA provisions are scarce
  - **Include establishing allowable uses and disclosures, implementing "appropriate safeguards," reporting breaches to the covered entity, ensuring agents and subcontractors follow suit and cooperating with investigations**

What Do BA Requirements Really Require?

- Terminology is vague, definitions may come in the future
- Must determine on our own the reasonable steps for a BA to take to work effectively with covered entities
- HIPAA regulations can be expected to create minimum “best practices” that all organizations can be expected to follow
- What to do?



Privacy Certification for Business Associates

- A joint initiative of NCQA and JCAHO
- A voluntary, private evaluation mechanism to provide business associates with a method of demonstrating satisfactory assurances of PHI protections to covered entities

PRIVACY CERTIFICATION FOR BUSINESS ASSOCIATES

Proposed Standards

- Closely track HIPAA privacy regulations
- Also include security requirements required by privacy
- Developed with input from multistakeholder Advisory Committee
- Categories include:
  - **Administration**
  - **Use and Disclosure**
  - **Individual Rights**

Use the Same Framework

- In creating our program, we asked the questions:
  - **How can the BA "back-up" the provisions of the BA contract?**
  - **What areas of a BA/covered entity relationship not addressed in the contract?**
  - **What processes must BAs have, no matter**
  - **How do you comply with differing covered entity requirements?**
  - **To what standard do you hold BAs?**

Basic BA Requirements

- Create infrastructure for PHI protection
- Determine routine business needs involving use, disclosure and storage of PHI
- Implement policies, procedures and processes for those routine business needs
- Coordinate with covered entities to determine unique needs
- Monitor, test, revise and refine processes over time
- BAs should be expected to meet same standards as covered entities, when performing the same functions

Creating Infrastructure

- Analyze business processes
  - **Where is PHI coming in from covered entities?**
  - **How is PHI being transmitted to covered entities, agents, subcontractors and workforce members?**
  - **How/where is PHI stored?**
  - **Can PHI be inadvertently sent during routine business processes?**
- Gaps? – close them
- Risk identified? – set up plan to deal with them

Creating Infrastructure - II

- Create Infrastructure to protect PHI
  - **Determine documentation requirements for the BA's processes**
  - **Set up physical and electronic access controls**
  - **Set oral PHI standards**
  - **Implement procedures for visitors**
  - **Create process to identify and mitigate PHI protection breaches**
  - **Set sanction policy for those breaches**

Creating Infrastructure - III

- Train staff on general requirements
  - **Overall PHI/HIPAA training**
  - **Include basic privacy and security**
  - **Explain why this affects your business**
  - **Include all workforce members**
- Implement specific training
  - **Based on role, type of PHI accessed, uses and disclosures of PHI needed**
  - **Tailor to departmental/unit needs**
- Create reminder system

Setting Daily P&P

- Focus on areas of routine use and disclosure of PHI
- Establish policies, procedures and processes to handle
- Set minimum necessary standards for internal uses and disclosures to agents and subcontractors
  - **May need to adapt for specific covered entity requirements**

Authorizations

- Determine if any routine business needs require authorizations
- If so, work with covered entities – who is responsible for obtaining?
- If covered entity responsible, BA should set up process to check whether authorization in place before disclosing
- If BA responsible, create authorization form and process for ensuring they are obtained when needed

Consumer/Individual Rights

- Individuals can access PHI, and request amendments, restrictions, confidential communications and accountings of disclosures
- BAs, depending on business processes, will have to deal with at least some of these
  - **Accountings of disclosures**
  - **Restrictions on use/disclosure agreed to by covered entity**

Consumer/Individual Rights - II

- Analyze business processes
  - **Does the BA contact consumers?**
    - **May get requests directly – where do you send them?**
    - **Confidential communications – how do you account for these?**
  - **How will restrictions on use and disclosure affect BA's processes?**
    - **Do you have a system to track and handle these – when agreed to by covered entity?**

Consumer/Individual Rights - III

- Analyze business processes
  - **Does the BA hold any portions of the designated record set?**
    - **How will BA provide access?**
    - **How will amendments be incorporated?**
    - **How will amendment denials be incorporated?**
  - **Does the BA disclose PHI?**
    - **How are disclosures tracked?**
    - **How will accountings be generated?**

Consumer/Individual Rights - IV

- Coordination is the Key
  - **Work with covered entities to determine which organization is responsible for different aspects of consumer rights**
  - **Set up processes accordingly, remembering**
    - **The covered entity could disappear tomorrow – what happens if the BA is the only holder of the PHI?**
    - **Even if BA does not directly deal with consumers, covered entity decisions on restrictions, amendments and other rights can affect BA's business**

Contracts/Agreements

- Covered entities responsible for obtaining contracts/agreements
- BAs can help by internally tracking:
  - **Are there existing covered entity clients/customers without contracts at all?**
  - **When are contracts up for renewal?**
    - **Before or after April 2004?**
  - **Which covered entities have contacted the BA with a BA contract or addendum?**
- Should the BA have its own contract?

Contracts/Agreements - II

- Study contract provisions
  - **Are there any that will interfere with routine business operations?**
  - **Are there other options to provide same protection but streamline BA's processes?**
  - **Are there areas covered entity should have included but didn't?**
- Set up system to alert staff to specific covered entity requirements

Questions?

PRIVACY CERTIFICATION FOR BUSINESS ASSOCIATES