The 6th National HIPAA Summit West

Department of Veterans Affairs (VA)

Veterans Health Administration (VHA)

Business Associate Audit Program

James "Mickey" Gwyn, MA, CIPP/G
Business Associate Program Manager

C. David McDaniel, CIPP/US, CIPP/G, CIPP/IT, CHPS
VHA Privacy Compliance Assurance Officer

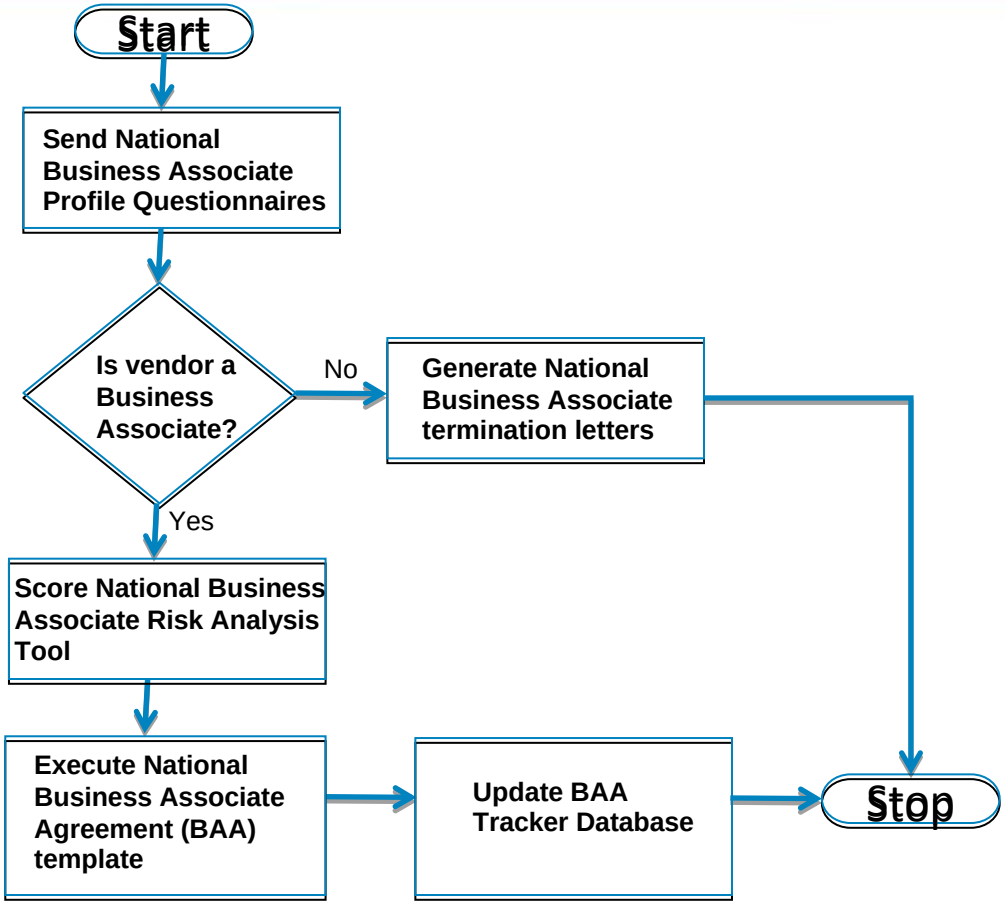
October 10, 2012

VA HEALTH CARE Defining EXCELLENCE in the 21st Century

Business Associate Audit Program

- VHA is committed to protecting Veteran data and keeping Veterans safe from identity theft or data loss
- Business Associates, often Veterans themselves, sought feedback on how they could better protect Veteran data as partners in health care delivery
- The Health Information Technology for Economic & Clinical Health (HITECH) Act requires covered entities to be more actively engaged with their Business Associates
- VHA strives to reduce data risks when supplementing VHA health care functions with external resources

Business Associate Agreement (BAA) Process



Business Associate Profile Questionnaire

- 23 individual questions
- Sample Questions
  - Do your services involve the use or disclosure of VHA's Protected Health Information (PHI)? (PHI includes patient identifiers such as name, social security number and address)
  - Does your company access, use or encounter VHA PHI outside of a VHA facility?
  - List the names of the VA Medical Centers, Program Offices or VISNs that receive the services noted
  - Does your company engage subcontractors in services provided to VHA under your Business Associate Agreement?
    - If you answered Yes, do you have a specific, documented chain of custody agreement that requires the subcontractor to meet the requirements set forth in your BAA with VHA?

Business Associate Profile Questionnaire

- Sample Questions
  - Does your company have direct contact with VHA patients?
  - Does your company have an assigned Privacy Officer or Compliance Officer?
  - Has your company ever been involved in a data breach involving VHA PHI?
  - Has your company developed and documented policies and procedures that explain safeguards to prevent use or disclosure of PHI not authorized by the
  - BAA? *(Specifically policies related to Privacy, Security and Records Management)*
  - Does your company have any other classification, other than Business Associate, as defined under the HIPAA Privacy and Security Rules? (*e.g., Covered Entity, Hybrid Entity, etc.)*

Business Associate Risk Analysis Tool

- Questionnaire reviewed for completion
- Answers given a weighted score
- Scores based on level of risk associated with response
- Total of all scores determines risk level

Business Associate Risk Analysis Tool

Data in Profile	Risk Score	Company Score
Does your company access VHA Protected Health Information (PHI) outside of a VHA facility? (Including PHI that has been disclosed to your company by VHA)		
YES		
NO		
How is VHA data accessed? (Select all that Apply)		
a. Electronic Means of Access:		
i. VPN		
ii. Interconnection		
iii. Direct Access to VHA		
iv. Other		

Business Associate Risk Analysis Tool

Data in Profile	Risk Score	Company Score
Does your company have **direct** contact with VHA patients?		
Company has direct contact with VHA Patients		
Company does not have direct contact with VHA Patients		
TOTAL RISK SCORE		

Moderate Risk	
High Risk	
Very High Risk	
Critical Risk	

Determining Business Associates For Auditing

- Business Associates ranked by risk score
- Business Associates further sorted by services provided
- Collaboration with VHA Privacy and Security offices
- Selected audit determined by evaluating risk analysis score, services provided, location and previous incidents collectively
- Initial email notification to Business Associate and handoff to Privacy Compliance Assurance

Why does VHA Privacy Compliance Assurance (PCA) Conduct these Assessments?

- VHA Privacy Office has a PCA organization
- PCA has conducted internal privacy assessments since 2002
- PCA already had:
  - Data-collection tools
  - Interview processes
  - Existing business processes to manage assessments
  - Trained compliance specialists
  - Reporting tools and processes
  - Credibility

Development of Evaluation Tools

- Processes and tools for conducting evaluations of VHA health care facilities
- Tool scalability to a broad spectrum of Business Associate services
- Collaboration between Privacy and Security functions internally
- Processes and tool formulas translated well and did not have to be re-created for the Business Associate Audit process

What to Expect in Logistics and Deployment

- Recommended Assessment Deployment
  - One-day evaluation
  - Review policy
  - Evaluate Privacy and Security practices
  - Physical review of operations
- Business Associate Work Location: Key to Success
  - Delivery location is often different than headquarters location
  - Business Associate point-of-contact is usually in headquarters location
  - Virtual workforce is prevalent which requires pinning down where the work is actually being conducted
- Know your Business Associate's services
  - Be prepared to learn about the various industries that serve you
  - This can be a learning curve for your staff conducting assessments

What to Expect in Logistics and Deployment (Cont'd)

- BAA signatories are generally NOT the vendor's Privacy and Security experts or managers who lead the specific services provided under the agreement
  - Make sure you have the right points-of-contact
- Legal, Security and/or Privacy experts may not reside in the same location where services are rendered
- The unknown can make your Business Associate uneasy so plan to reassure them that your intent is to partner with them

Staffing Challenges

- VHA manages Business Associates at both national level and local level
  - Local defined as a Business Associate serving only one VHA hospital or VHA health care system
- PCA focused on national-level Business Associate relationships
  - VHA has over 400 of these national agreements
  - Local agreements covered by facility privacy officer
- Security personnel needed for some, but not all assessments
  - Some vendors manage the whole lifecycle of VHA's PHI
  - Some do not need PHI at all, but have unmonitored accessibility to it (e.g., shredding vendors, janitorial services who work after-hours, etc.)
- Teams of two required at a minimum to provide corroboration of events and findings
- Remediation support staff assigned to reconcile any findings

Preparing Business Associates for Assessment

- Take the time to listen to the concerns of the Business Associate and reassure them that the assessment process is about continuing and improving our partnership
  - Answer questions during initial planning conversations
  - Describe the selection process for audits
- Provide the Business Associate with the questions in advance
  - It helps them better understand the process and how to prepare
  - It helps you sort out any scope issues before you get on-site
- When conveying findings of non-compliance, give them some idea of what would satisfy your expectations as to what constitutes compliance
  - Formal out-briefing with summary report provided at the end of the assessment
  - Remediation timeframe recommended (usually 90 days from assessment)

Managing Unexpected Experiences

- VHA requires all Business Associates to be located and provide their services in U.S. jurisdictions
  - Business Associates often do not think about off-shoring as problematic
- Some vendors have signed agreements and are not Business Associates. They enter into the agreement because they do not want to lose VA business. Ways to correct this are:
  - Clarifying relationship during initial negotiations for the agreement
  - Clarifying during logistical discussions to double-check that they are in fact a Business Associate
  - Open and clear communication throughout all interactions
- Some hybrid HIPAA-Covered-Entities may be providing services that are delivered by their non-covered functions, but the vendor has not made a distinction in policies and practices

Remediation Activities

- Remediation of findings is critical since you are now aware of any non-compliance as a result of the assessment
  - Track performance and provide feedback on what you consider
  - Provide samples so the Business Associate can conceptualize expectations
- Most vendors are very open to remediation because they want a competitive edge in health care
- The assessment is just a snapshot in time. Be careful about certifying compliance. VHA does not “advise” or “consult” with vendors on solutions
- Be prepared to dissolve the Business Associate relationship if the vendor is doing things that are non-compliant and they will not correct the issue

What to Do and Not Do With the Data

- Do keep detailed documentation to meet HIPAA compliance monitoring requirements and retain all records.
- Do analyze the findings and keep your organization informed of the risks associated with using outside resources
- Do manage remediation efforts
- Do let the assessment data inform policy decisions as to which kinds of services are low risk when outsourcing and which ones may need to be kept in-house
- Do not share assessment information on Business Associate with others. Some vendors want to know how their peers score on assessments
- Do not provide certifications of compliance as a result of the assessment

Pleasant Surprises

- Most Business Associates score very well on assessments
- Most are very open to changing to meet the requirements
- The Business Associates want to do the right thing and is willing to be good partners in confidentiality of our patients' PHI
- We learned that using vendors can become very complex
  - The assessment process helps to improve our understanding of our Business Associate's roles in our organization

Future Plans to Maximize Business Associate Relationships

- Gain a better understanding of the services provided and a clearer picture of how to scale the assessment process for a better fit by vendor type
- Build a robust web-based support site for Business Associates to provide them with information on:
  - The assessment process
  - Why they were selected for an assessment
  - Remediation expectations
  - Samples of compliant policies, processes and other tools that would help them conceptualize what compliance looks like from our perspective
- Improve the local Business Associate monitoring
- Develop strong strategies for responding to data breaches in Business Associates to minimize any damage to our patients in the event of a breach

Questions

Contacts:
James “Mickey” Gwyn, Business Associate Program Manager
james.gwyn@va.gov (615) 898-1512

C. David McDaniel, VHA Privacy Compliance Assurance Officer
david.mcdaniel@va.gov (202) 360-1475