Mind Your Own Business... Associates

Tips for Creating and Implementing a Successful Business Associate Assessment Program

Sharon A. Anolik, Esq., CIPP
Director of Corporate Compliance and Ethics
Chief Privacy Official
Blue Shield of California

CMS & NIST HIPAA Security Rule Workshop
January 16, 2008

Overview

- Legal Basis/Minimizing Risk
- Pre-Assessment Preparation
- Types of Assessment Programs
- Assessment Approaches
- Conducting the Assessment
- Post-Assessment Work

“But we have a signed agreement.”

- HIPAA does not directly require a CE to develop an assessment program, but Sec. 164.502(e)(1)(i) does require a CE to obtain “satisfactory assurance that the BA will appropriately safeguard the information.”
- CEs must implement reasonable and appropriate administrative, technical and physical safeguards to “insure the integrity and confidentiality,” and protect against “threats or hazards to the security” of health information.
- Organizations need to understand how their member data is shared, transmitted, created and stored by their BAs and how it is safeguarded…

To truly mitigate risk, a signed BAA should be the beginning – not the end – of your privacy and security obligations.

Do your homework

- Identify which of your BAs are key business partners or sources of significant liability.
- Develop selection criteria, and clearly explain why BAs are being chosen for review.
- Do your homework prior to conducting the assessment.
  - Understand what your BA does for your organization.
  - Review the underlying contract.
  - Identify areas where your BA's compliance approach or processes differ significantly from those adopted by your organization.
  - Note prior security problems, remediation, mitigation and compliance history.
  - Review provisions governing BA audit rights and access to BA facilities and policies/procedures.
- Involve the business unit that the BA primarily serves.
- Leverage findings from recent reviews or audits from other internal departments.
- Check with your organization's legal advisors regarding Attorney-Client privilege for both the assessment itself and the report of your findings.

Types of Assessment Programs

- In-House
  - – All monitoring and assessing of BA compliance handled internally within your organization.
- Outsourced
  - – Contract your assessment program to an external consultant/3rd party.
- Hybrid
  - – Retain a third party to develop an assessment program which is then implemented and supported by your organization.
- Shared
  - – Multiple CE's work together to:
    - evaluate a common BA
    - hire a 3rd party to perform an assessment on their collective behalf

Assessment Approaches

DESK-LEVEL assessment: completed within your office without an on-site visit to the BA.

Benefits

1) Reduces audit costs
   - No travel costs
2) Ease on staff schedules
   - Interviews done via phone
3) Are normally quicker to complete, resulting possibly in more completed audits

Limitations

1) Limited to the specific information provided by the BA
2) Phone interviews do not always produce the same results as those done in person
3) May still require an on-site assessment at later time

ON-SITE assessment: desk review followed by an on-site assessment at the BA's location.

Benefits

1) Indicates to the BA that you take compliance seriously
2) Enables you to observe actual operations, rather than relying on PnP and process documents
3) Provides CE with more of an overall sense of compliance than a desk-level assessment

Limitations

1) Increases audit costs
2) Cannot complete as many audits because of cost and time constraints
3) Not as flexible to change once arrangements have been set

“Look Ma – no hands!”

- Confirm a meeting of the minds internally, and set BA expectations accordingly.
  - –Define roles/responsibilities, tools to be used, quality expectations, and assessment scope.
- Develop a schedule/timeline for the assessment, including due dates.
- Define your methodology:
  - – Focus on a specific BA agreement requirement or HIPAA provision, and follow the BA process for compliance/response; or
  - – Focus on a BA business area, and map their functions back to the requirement/provision.
- Leverage or develop standard templates (communications, agenda, document requests, interview questionnaire, corrective action plan, checklists, root cause analysis chart, etc.).
- Questionnaire Tips:
  - – Cite the specific provision on which the question is based.
  - – Structure the questionnaire so that root cause analysis can be easily conducted.
  - – Use the questionnaire to capture responses from interviews, documentation review, and BA responses.
- Meet with employees at various levels within the company.
- Confirm that personnel selected to respond to questionnaires or participate in interviews have appropriate knowledge and authority.

Findings, Fixes & the Future

- Call out both recurring and isolated findings in your Assessment notes. Highlight areas that may be systemic.
- In your final report, clearly identify findings and quantify the impact of each issue.
- Identify areas where the BA's compliance approach, policies and procedures, or other processes differ significantly from those adopted by your organization.
- Ensure the final corrective action plan includes timelines and identifies the parties responsible for completion.
- Offer recommendations on how to rectify the issues.
- Plan a follow-up assessment, if necessary, to ensure corrective action plan implementation.
- Monitor BA compliance.
- Debrief the Assessment and identify areas for improvement.

Contact Information

blue of california

Privacy Office
P.O. Box 272540
Chico, CA 95927-9914
(w) 888.266.8080
(f) 800.201.9020
(e) blueshieldca_privacy@blueshieldca.com

Sharon A. Anolik, Esq., CIPP
Blue Shield of California
Director of Corporate Compliance and Ethics
Chief Privacy Official
(w) 415.229.6903
(e) sharon.anolik@blueshieldca.com


blue of california