

Mind Your Own Business... Associates

Detailed Guidance 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

HCCA Managed Care Compliance Conference

Overview

Today's Environment at a Glance

Assessment Program Choices

Performing The Assessment

References

Q & A

Contact Information

The Risks, The Rules & The Reality

Quantifying Liability

30% of reported data breaches involved an entity's external partners.¹

50% of surveyed healthcare organizations reported breaches
by external partners.¹

Lawsuits

Reputation

Monetary Damages

Statutory Provisions

Under HIPAA Administrative Simplification, Covered Entities (CEs) must:

- understand how their member data is shared, transmitted, created and stored by their Business Associates (BAs).
- 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. (§ 164.502 (e)(1)(i))

Your organization may be liable for your BA's failure to provide safeguards if there was a known activity or pattern resulting in a breach or violation and you failed to take reasonable steps. (§ 164.504(e)(1)(ii))

- What are reasonable steps?
 - mitigation
 - termination
 - reporting
- "known" = "should have known" ?

Risk Management

HIPAA does not directly require a CE to develop an assessment program, but it does require a CE to obtain satisfactory assurance that the BA will appropriately safeguard the information.

CEs must ensure their BA contracts reference statutory and regulatory directives on safeguarding the confidentiality, integrity and availability of PHI/ePHI.

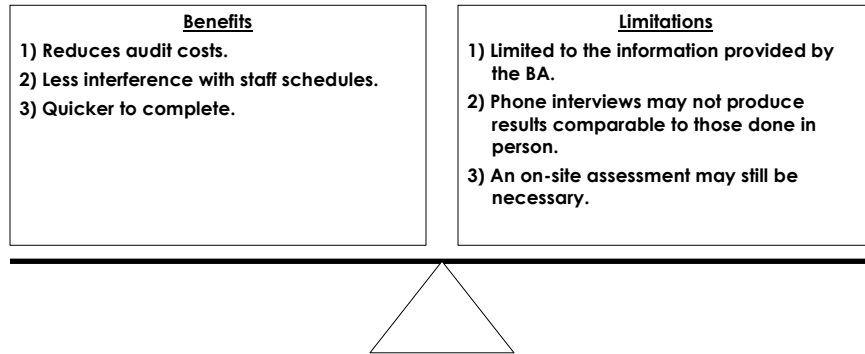
To truly mitigate risk, a signed BA agreement should be only the beginning of an organization's privacy and security obligations... not the end.

Choose the program
that works for you.

Assessment Approaches

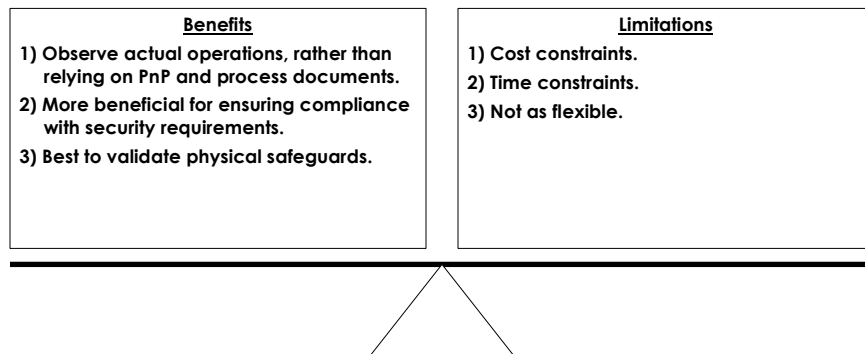
Desk Level Assessment

Completed within your office, without a visit to your BA's facility.



On-Site Assessment

A visit to the BA's physical location, likely including an in-depth desk-level review prior to the on-site visit.



Types of Assessment Programs

In-House

All program development and implementation handled within your organization.

Pros

- More control over resources, budget, timeliness, scope.
- Ensures consistency with other internal audit programs.
- Increases chance of getting business area buy-in.

Cons

- Difficulty finding knowledgeable and experienced people.
- Time constraints of existing staff.

Outsourced

Assessment program developed and implemented by an external party.

Pros

- Quick and easy to implement.
- Benefit from expert's industry knowledge and tools.
- Doesn't pull staff away from other responsibilities.

Cons

- Scope of assessment might be too narrow.
- Cost may limit the number of assessments that can be completed.
- Program not customized.
- CE lacks total control.

Hybrid

An externally developed assessment program implemented and supported by your organization.

Pros

- Templates, formats and tools customized specifically for your organization.
- After development, the program is owned and executed by your organization.

Cons

- Still requires significant time commitment from staff.
- Cost may limit the number of assessments that can be completed.

Shared

Multiple CEs work together to evaluate a common BA, or hire a third party to perform an assessment on their collective behalf.

Pros

- Reduces the impact to CE staff.
- Out-of-pocket costs lower.

Cons

- Assessment may not be able to address unique issues of participating CEs.

The Assessment

Determining Population

Develop selection criteria.

Create a short list.

- identify key business partners
- identify sources of significant liability

Provide justification for the BAs chosen for assessment.

Internal Buy In

Contact internal business areas.

- senior management
- department(s) served by BA

Consult legal advisors regarding Attorney-Client privilege.

- the assessment itself
- the report of assessment findings

Do Your Homework

- Prior to conducting the assessment, know:
 - the similarities and differences among your BA agreements
 - your assessment plan and processes (even if it has been out-sourced)
 - what the BA does for your organization
 - your underlying contract with the BA
 - provisions governing assessment rights, and access to facilities, PnPs, and process documents

What To Look For

Where do your BA's compliance processes differ significantly from yours?

If and how the BA is reasonably and appropriately safeguarding your PHI.

Does the agreement reflect the current risk environment?

Compliance with reporting requirements.

Are special offshoring issues addressed?

Do the BA's agreement, processes documents and actual operations align?

Are privacy and security responsibilities well defined and coordinated?

Note prior problems, remediation, and mitigation.

Nuts & Bolts

Define the assessment methodology:

- focus on a specific BA agreement requirement or HIPAA provision, and follow the BA process for compliance/response, or
- focus on a business area, and map functions back to the requirement/provision

Define roles/responsibilities, tools to be used, quality expectations, and assessment scope.

Develop a schedule/timeline, including due dates.

Detail a communication strategy.

Preparation

Confirm BA participants have appropriate knowledge and authority.

Develop or leverage standard templates, including:

- communications
- document requests
- interview questionnaire
- corrective action plan
- checklists
- root cause analysis chart
- reports

Leverage recent reviews or audit findings.

Questionnaire Tips

Cite the provision on which the question is based.

Structure for easy root cause analysis.

Capture and identify responses from:

- documentation
- BA written responses
- interviews

Use open-ended questions.

Provide questionnaire completion instructions.

Decide whether to use a scoring or non-scoring checklist.

Findings

Give background (why was this BA chosen for assessment).

Calibrate findings and observations with internal reviews.

Categorize and clearly identify findings, then quantify the impact of each issue.

In assessment notes:

- include isolated findings
- call out recurring findings
- highlight areas that may be systemic
- identify areas where compliance approach, PnPs, or other processes differ significantly from yours

Fixes

Debrief appropriate internal stakeholders.

Identify internal areas for improvement.

Enlist business unit support for:

- delivery of report
- implementation of recommendations

The corrective action plan should:

- include timelines
- identify responsible parties
- establish regular meetings to review status

Offer recommendations on how to rectify issues.

The Future

Require a BA to meet certain standards before entering into a contract.

Impose performance standards and penalties.

Monitor BA compliance.

Ensure your BAs know who to contact in your organization when a privacy or security incident occurs

- during and outside of normal business hours

Share best practices.

Pause to Assess Yourself

Does your own organization...

- ensure an appropriate BA agreement is signed prior to sharing data or PHI?
- know its obligations as identified in the BA agreement?
- have clearly defined and coordinated privacy and security department responsibilities?
- ensure your core privacy and security PnPs and processes are consistently implemented and applied wherever your PHI is?
- know how to reach the Privacy or Security Official in the event of a breach?

Extras

References

Glossary

- Business Associate (BA): a person or entity that performs certain functions that involve the use or disclosure of protected health information, or provides services to, a covered entity.
- Covered Entity (CE): a health care provider that conducts certain transactions in electronic form, a health care clearinghouse, or a health plan.
- Policy and Procedure (PnP)

Footnotes


1. Ponemon Institute, 2006

Additional Resources

- HIPAA Administration Simplification Rules
 - Privacy: Sec. 164.502(e) and (f)
 - Security: Sec. 164.306, 164.308(b), 164.314(a)

Q & A

Contact Information

blue  of california

Privacy Office

Mailing address: PO Box 272540, Chico, CA 95927-9914

Phone: 888.266.8080

Email: blueshieldca_privacy@blueshieldca.com

Sharon A. Anolik, Esq., CIPP


Blue Shield of California

Director, Corporate Compliance and Ethics

Chief Privacy Official

415.229.6903

sharon.anolik@blueshieldca.com

blue  of california

31

blueshieldca.com