MIND YOUR OWN BUSINESS …
ASSOCIATES: CONDUCTING BAA AUDITS

HIPAA SUMMIT XIII
September 26, 2006 1:30 PM

Steven Fleisher, Esq.
Senior Director, Compliance &Privacy
Blue Shield of California

Sharon A. Anolik, Esq.
Privacy Official
Blue Shield of California

topics

legal requirements
- HIPAA
- other legal requirements

risk management
- benefits to having an established BA audit program
- risk from knowing more than you want to
- a few ways to help minimize risk

audit types and approaches
- desk audit
- on-site audit
- defensive auditing
- creating and using standard documentation
- audit checklist tips
- audit questionnaire tips
- in-house audit program
- outsourced audit program

ruminations
- privacy thoughts
- security thoughts

questions & comments

contact information

legal requirements

HIPAA Administrative Simplification

Standards of Privacy of IIHI

§164.502. Use and Disclosures of Protected Health Information: General Rules

(e)(1) Standard: disclosures to business associates.	
(i)	"A covered entity may disclose protected health information to a business associate and may allow a business associate to create or receive protected health information on its behalf, if the covered entity obtains satisfactory assurance that the business associate will appropriately safeguard the information."
(iii)	"A covered entity that violates the satisfactory assurances it provided as a business a business associate of another covered entity will be in noncompliance with the standards, implementation specifications, and requirements of this paragraph and §164.504(e).
(e)(2) Implementation specification: documentation.	
	"A covered entity must document the satisfactory assurances required by paragraph (e)(1) of this section through a written contract or other written agreement or arrangement with the business associate that meets the applicable requirements §164.504(e)."

HIPAA Administrative Simplification

Standards of Privacy of IIHI

§164.504. Use and Disclosures: Organizational Requirements

(e)(1) Standard: business associate contracts.	
(ii)	**"**A covered entity is not in compliance with the standards in §164.502(e) and paragraph (e) of this section, if the covered entity **knew of a pattern of activity or practice of the business associate that constituted a material breach or violation** of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful: (A) Terminated the contract or arrangement, if feasible; or (B) If termination is not feasible, reported the reported the problem to the Secretary." (emphasis added)

HIPAA Administrative Simplification

Standards of Privacy of IIHI

§164.504. Use and Disclosures: Organizational Requirements

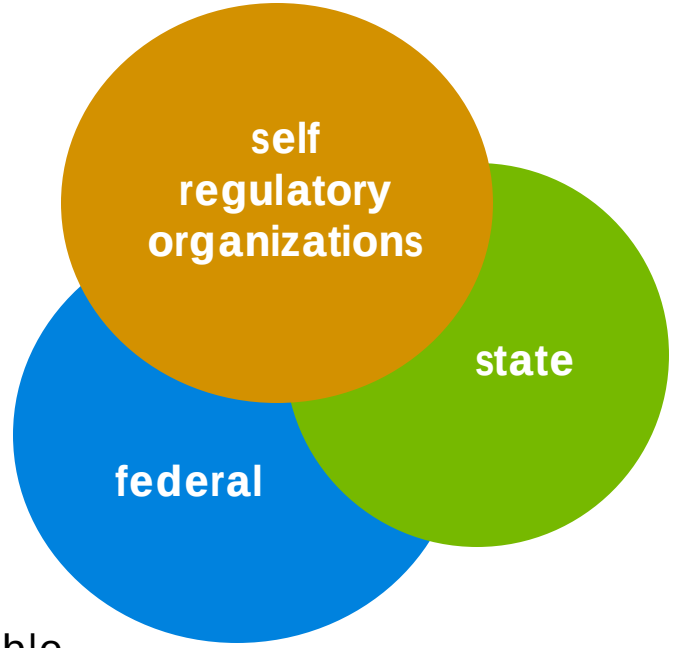
(e)(2) Implementation specifications: business associate contracts.

(ii)

Additional business associate (BA) requirements:

- Do not use or further disclose PHI
- Use appropriate safeguards to prevent use or disclosure
- Report to the CE any use or disclosure
- Ensure that BA agents agree to the same restrictions that apply to the BA with respect to such information
- Make available PHI (§164.524_
- Amend or incorporate amendments to PHI (§164.526)
- Make available a disclosure report (§164.528)
- Make internal practices, books and records relating to use or disclosure of PHI received or created for the covered entity to DHHS to determine the CE's compliance
- Return or destroy PHI at the termination of the contract, if feasible; or, extend the protections of the contract to the information

other legal requirements



State and Federal Requirements

- California Medical Information Act (CMIA)
  (CA Civil Code §[51])
- 33 states have different data breach notification laws, and a federal law has been proposed
- New trend from the FTC holding businesses responsible for the conduct of their business partners

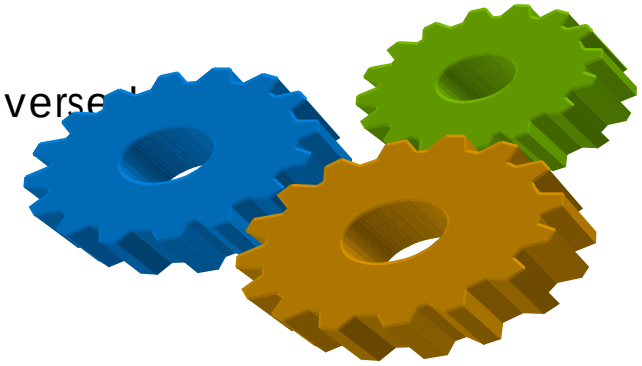
Self-Regulatory Organizations

- Privacy Certification for Business Associates (PCBA)
- TRUSTe
- American Hospital Association (AHA)

risk management

benefits to having an established BA audit program

- Knowing your business associates (BA) and how they really operate
- Really understanding your business associate agreement (BAA)
- Setting the tone internally — and with the BA — that you take privacy seriously
- Decreasing likelihood of PHI mishandling by the BA
- Decreasing risk of public relations misstep
- Documenting internal workflows on how to interact with a BA
- Knowing how to comply as a BA when roles are reversed
- Showing good faith effort to safeguard PHI



risk from knowing more than you want to

- Duty to act: mitigate, terminate or report (164.504(e)(1))
- Duty to disclose and notify others under state law
- Paper trail of known breaches and violations
- Remember what you don't know can hurt you
- If there is a breach, you and your BA might get sued
- If there is a breach, you and your BA could receive bad press and suffer harm to your reputation

a few ways to help minimize risk ...

- Clearly identify reporting requirements in your BAA
  - Purpose, content, format, and frequency
- Make your BA aware of your organization's BA audit process
  - Ensures understanding of the audit process, checklists that will be utilized, and measurement expectations
- Share best privacy practices with BA to encourage compliance
  - Promotes open communication between the BA and covered entity
- Track who in your organization is responsible for the relationship between the you (as the CE) and BA
- Keep on top of all the services that your BA is providing for you
  - Reduces the opportunity for unexpected privacy issues

audit types and approaches

desk-level audit

Limitations

1) Limited to the specific information provided by the BA

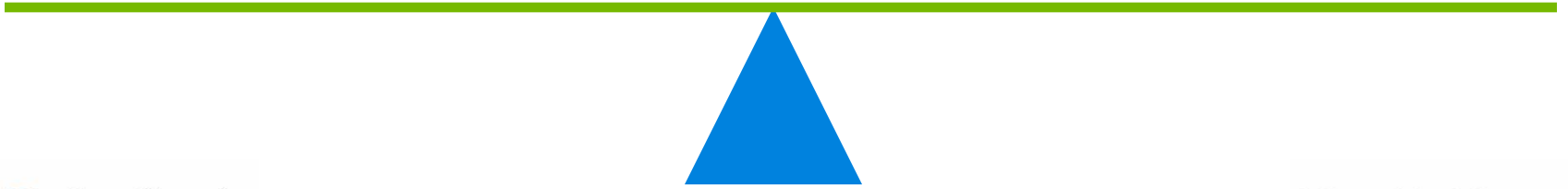
2) Phone interviews do not always produce the same results as those done in person

Benefits

1) Reduce 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



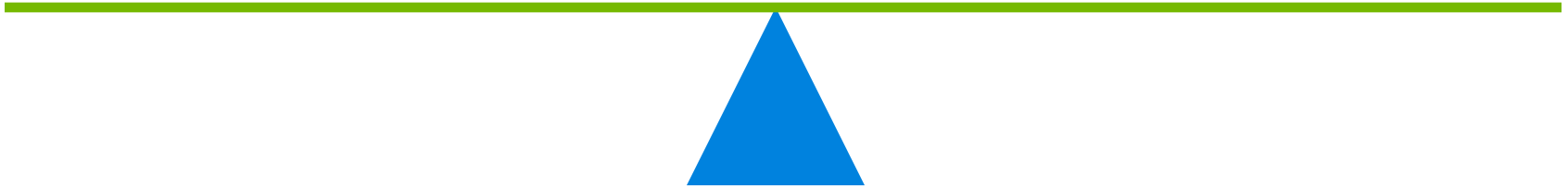
on-site audit

Limitations

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

Benefits

1) Could be perceived by the BA that the CE is taking compliance seriously
2) Can observe actual operations, rather than relying on procedure documents
3) May provide more of an overall sense of compliance than a desk-level audit



defensive auditing

When privacy incidents arise with BAs, follow your established and documented incident response program which should include the 5 “fies”

- **Identify** and define the privacy issue
- **Quantify** the impact of the privacy issue
- **Rectify** and mitigate corrective action
- **Solidify** and document the appropriate steps to resolve
- **Notify** appropriate stakeholders

creating and using standard documentation

- Develop a strong and well thought out BA audit plan for your organization which documents roles and responsibilities, quality measurements, what primary areas will be included the audit and why
- Keep BA audit plan current with company policies and department workflows
- Get buy-in from the internal business areas impacted by your BA audit plan
- Look to see if there are any standard documentation formats that can be followed both internally and externally
- Be consistent in using your documentation with different BAs
- Include the following standard templates in your audit program: agenda, interview questionnaire, checklists, initial communications, reports, corrective action plan, root cause analysis chart

audit checklist tips

- Track the language of your BAA when developing a checklist
- Understand the underlying agreement between the BA and the CE in order to understand exactly what the BA does for you as the CE
- Determine if your organization wants to use a scoring or non-scoring checklist
- Use open-ended questions on the interview questionnaire to solicit more information
- Make sure that the person who is responding to your checklist or interview questionnaire is the appropriate person (with knowledge and authority) at the BA
- Structure the checklist so that root cause analysis can be easily assessed
- Provide instructions on how to use the checklist and what is expected from the BA, including due date for responses

audit questionnaire tips

- Cite the applicable HIPAA section next to the question it corresponds with
- State your questions in easy-to-understand terms
- Allow space on your questionnaire to enable a respondent to provide additional information. Example:

Privacy Rule §	Question	Response
164.526(b)(2)	Does the BA have a document process to handle amendments to member PHI records?	Yes. The process is documented and employees have been trained. Attached is a copy of amendment workflow.

in-house audit program

Benefits

1) Control over budget, scope, templates, everything
2) May increase consistency with other internal audit programs
3) Increase chance of getting business area buy-in

Limitations

1) Finding qualified people
2) Lack of initial procedures and documentation
3) Time constraints of existing staff

out-sourced audit program

Benefits

1) “Audit Program in a Box”
2) Benefit from expert’s industry knowledge and tools
3) Doesn’t pull your staff away from their other responsibilities

Limitations

1) Scope of audit services purchased might be too narrow
2) Cost, which limits the number of audits that can be completed each year
3) 3rd party may not conduct the audit the way you would have

ruminations

privacy thoughts

- Since the implementation of HIPAA, many organizations have not gone back to review their policies, workflows and relationships.
- The auditing of BAs has not become an industry standard.
- Possible increased scrutiny about what CEs are doing to ensure privacy of member PHI with the implementation of the HIPAA Enforcement Rule.
- Juggling federal, state and self-regulatory requirements are a challenge for CEs and BAs.
- Push-back from internal business areas regarding ensuring that an appropriate BAA is signed prior to sharing data.
- The Court of Public Opinion is in session and various organizations are watching entities closely to see how they handle member PHI.

security thoughts

- The scope of responsibilities of privacy and security departments within an organization, if they are separate, are not always well defined or well coordinated.
- On-site audits may prove to be more beneficial for ensuring compliance with security requirements.
- Organizations often do not look to improve the initial solutions that were implemented in their efforts to become compliant with HIPAA (e.g., encrypting computer workstations and laptops).
- Global events may impact an organization's security of computer hardware and employees do not often realize the ramifications until it is too late (e.g., checking laptops on to a plane versus being able to carry them on).

questions?

contact information

contact information

Blue Shield 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

Steven Fleisher, Esq.
Senior Director, Compliance & Privacy
(w) 415.229.5914
(e) steven.fleisher@blueshieldca.com

Sharon A. Anolik, Esq.
Privacy Official
(w) 415.229.6903
(e) sharon.anolik@blueshieldca.com

thank you.

your privacy