



Alliance Collection Agencies, Inc.



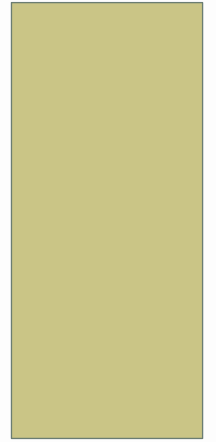
Healthcare Business Services, Inc.

**A PRACTICAL APPROACH TO:
HIPAA BREACH REPORTING
&
KEEPING A COMPLIANCE PROGRAM ALIVE**

Presented By:

Catherine Colyer, Corporate Counsel and Compliance Officer

PART ONE



HIPAA BREACH REPORTING

THE PLAYERS

- Covered Entities (CE)
- Business Associates (BA)
- DHHS/OCR (investigation & enforcement)

HIPAA BREACH REPORTING

SB = Suspected Breach

Q

Do you work for a Covered Entity (CE)?

Q

Do you work for a Business Associate (BA)?

Q

Are you directly involved in some portion of the breach process in your organization?

REPORTING – INFORMATION FLOW

BA captures SB information



Conveys information to CE



CE makes breach determination



CE reports to DHHS if necessary

SUGGESTED TASK (CES AND BAS)

- Review your Business Associate Agreement
- Chart the differing requirements (notification, etc) into a quick reference guide
- Provide standard, written format, if necessary

WHAT DOES A BA NEED TO CONVEY TO A CE?

- **Objective Information** – Just the facts/write objectively
 - “The provider sent an itemized statement out to the wrong patient.”
- vs.
- “The caller stated that she had received an itemized statement for someone named Jane Patient.”

SUGGESTED TASK (CE)

- “breach” v. “suspected breach”
 - SB Notification Form
 - Internal Documents
 - Training
 - Casual Office Conversation
 - Lead By Example

SUGGESTED TASK (CE)

- Evaluate for Objectivity/Fact-Based Writing
 - SB Notification Form
 - Internal Documents
 - Introduce the concept of the red herring

SUGGESTED TASK (BA)

- Review the method you use to notify your clients of suspected breaches
 - Standardized format?
 - Objective information only?
 - If email: is it secure?
 - If email attachments: are they in pdf form?
 - Confirmation of receipt/follow-up?

SUGGESTED TASK (BA)

- Who is writing SB notifications?
 - Who is the best writer in your organization?
 - Refresher training session for writers on how to write objectively

SUGGESTED TASK (BA)

- Quarterly Compilation Reports to Clients
 - Confirms receipt of all SB notifications
 - Identifies disclosure patterns
 - Provides an opportunity for joint problem-solving

WHAT DOES A BA NEED TO CONVEY TO A CE?

- **All** facts necessary to make an informed decision
 - Patient's name
 - Date of incident
 - Date of discovery
 - CE account number and facility name
 - Description of incident (narrative)
 - Type(s) of information disclosed (demographic, financial, clinical)
 - Mitigation
 - Root Cause Analysis
 - More?

Q

How many CEs are currently receiving all of those categories of information?

THE BOTTOM LINE

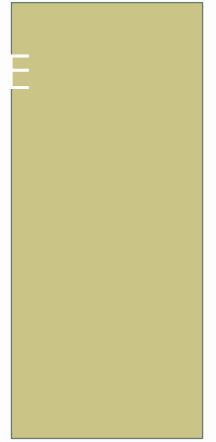
If a BA has not developed a sophisticated, comprehensive method for capturing the right information surrounding an SB incident, the BA is falling short of its duties under the law and the BA Agreement

But a BAs reporting role must have clear and definitive boundaries

WHAT SHOULD A BA **NOT** CONVEY TO A CE?

- Opinion
- Conclusions (including breach determination)
- Superfluous information

PART TWO



HCO COMPLIANCE PROGRAM

Year One

- Assembled a cross-company compliance team
- Created the proper foundation
- Compliance Officer
- Privacy Officer
- The big roll out!
(mandatory attendance)

Year Two and Beyond



WHAT IS THE FUNCTION OF THE CP NOW?

- Maintain Awareness of Compliance and of the CP
 - Use your CP logo
 - Regular recognition of extraordinary compliance behavior
 - Email blasts/compliance tips

Q

Another example of a way to maintain awareness of compliance and the CP?

SUGGESTED TASK (CE AND BA)

- Develop a “look” for your Compliance Program
 - Email blasts/compliance tips
 - Visuals throughout the company (ex: banners)
 - Tactile giveaways at training – become known for lively, informative training sessions

SUGGESTED TASK (CE AND BA)

- Identify recognition opportunities for compliance behavior
 - Performance evaluations
 - Newsletter/highlight a problem solved
 - Employee nominations (humor is a good thing)

WHAT IS THE FUNCTION OF THE CP NOW?

- Provide Ongoing Training
 - Annual compliance training (no repeats!)
 - Survey of managers to identify need/topics
 - Targeted training throughout every year
 - e-Training

CASE STUDY: TRAINING

Professional Development University

- Cross-company development team
- Naming of our “university”
- Course Catalog
- Weight Assignment (PDUs)
- Location for Record Keeping (including scores)
- Levels of Achievement
- Post-tests and Trainer Evaluations

Q

Will anyone share a suggestion for a creative or effective way to provide training?

SUGGESTED TASK (CE AND BA)

- Build Training Schedule for 2012
 - Survey management for needed training
 - Involve compliance team and identify top 3
 - Brainstorm on best format (large group, small group, live, virtual)
 - Post-tests are mandatory

WHAT IS THE FUNCTION OF THE CP NOW?

- To Ensure that the Compliance Team Matures
 - Reduce meeting frequency
 - Advisory role
 - Maintain organization and appropriate level of formality with the team (don't lose steam)
 - one-on-one projects with team members

SUGGESTED TASK (CE AND BA)

- Guide Compliance Team Into New Role
 - Hold interactive meeting with discussion questions
 - Administer CP maturity assessment - present results at next team meeting

WHAT IS THE FUNCTION OF THE CP NOW?

- Conduct Risk Assessments
 - Start with RA grid (multiple options, sample provided)
 - Identify interviewees – breadth and depth
 - Prepared Gap Analysis
 - Prepare Action Plan (with deadlines)
 - Identify Necessary Training

2011 Risk Assessments

<i>Risk Area</i>	Dimensions of Risk							Risk Score
	<i>Reviewed Last 3 Years</i>	<i>Past Audit Results</i>	<i>Size & complexity of area</i>	<i>Personnel Competency</i>	<i>Changing & New Regulations</i>	<i>Management Concerns</i>	<i>External Scrutiny</i>	
Using vendors for support or searches (<u>e.g.</u> , OSC has full access)								
Process for data changes to accounts (RP, SSN, DOB)								
Encrypted emails								
Proper scanning of documents to appropriate accounts.								

1 = Low Risk

3 = Neutral

5 = High Risk

SUGGESTED TASK (CE AND BA)

- Conduct Three Risk Assessments in 2012
 - Identification of Risk (spreadsheet provided)
 - Conduct Interviews
 - Conduct Gap Analysis
 - Prepare Action Plan (with deadlines)



Alliance Collection Agencies, Inc.



Healthcare Business Services, Inc.

THANK YOU

CATHERINE COLYER

CATHERINE.COLYER@ALLIANCE-
COLLECTIONS.COM



Check List for Business Associations

I. HIPAA Breach Reporting

- Review your Business Associate Agreement
- Chart the differing requirements (notification, etc) into a quick reference guide
- Provide standard, written format, if necessary
- Review the method you use to notify your clients of suspected breaches
- Who is writing SB notifications?
- Quarterly Compilation Reports to Clients

II. Compliance Program Maintenance

- Develop a “look” for your CP
- Identify recognition opportunities for compliance behavior
- Build Training Schedule for 2012
- Guide Compliance Team Into New Role
- Conduct Three Risk Assessments in 2012

Check List for Covered Entities

I. HIPAA Breach Reporting

- Review your Business Associate Agreement
- Chart the differing requirements (notification, etc) into a quick reference guide
- Provide standard, written format, if necessary
- “breach” v. “suspected breach”
- Evaluate for Objectivity/Fact-Based Writing

II. Compliance Program Maintenance

- Develop a “look” for your CP
- Identify recognition opportunities for compliance behavior
- Build Training Schedule for 2012
- Guide Compliance Team Into New Role
- Conduct Three Risk Assessments in 2012

PRISMA rating 1 through 5: (provided by ACA)

Maturity Level 1 → Policies

- Formal, up-to-date documented policies stated as “shall” or “will” statements exist and are readily available to employees.
- Policies establish a continuing cycle of assessing risk and implementation and use monitoring for program effectiveness.
- Policies written to cover all major facilities and operations agency-wide or for a specific asset.
- Policies identify specific penalties and disciplinary actions to be used if the policy is not followed.

Maturity Level 2 → Procedures

- Formal, up-to-date, documented procedures are provided to implement the compliance controls identified by the defined policies.
- Procedures clarify where the procedure is to be performed, how the procedure is to be performed, when the procedure is to be performed, who is to perform the procedure, and on what the procedure is to be performed.

Maturity Level 3 → Implementation

- Procedures are communicated to individuals who are required to follow them.
- Compliance procedures and controls are implemented in a consistent manner everywhere the procedure applies and are reinforced through training.
- Ad hoc approaches that tend to be applied on an individual or case-by-case basis are discouraged.
- Initial testing is performed to ensure controls are operating as intended.

Maturity Level 4 → Test

- Tests are routinely conducted to evaluate the adequacy and effectiveness of all implementations.
- Tests ensure all policies, procedures, and controls are acting as intended and they ensure the appropriate compliance level.
- Effective corrective actions are taken to address identified weaknesses, including those identified as a result of potential or compliance incidents or through alerts issued by FedCIRC, vendors, and other trusted sources.

¹ Program Review for Information Security Management Assistance is based upon federal requirements for compliance and acknowledged best data security practices.

PRISMA rating 1 through 5: (provided by ACA)

Maturity Level 4 → Test Continued.

- Self-assessments (a type that can be performed by agency staff, by contractors, or others engaged by agency management) are routinely conducted to evaluate the adequacy and effectiveness of all implementations.
- Independent audits such as those arranged by clients are an important check on agency performance, but are not viewed as a substitute for evaluations initiated by agency management.
- Information gleaned from records of potential and actual compliance incidents and from security alerts, such as those issued by software vendors, are considered as test results. Such information can identify specific vulnerabilities and provide insights into the latest threats and resulting risk.
- Evaluation requirements, including requirements regarding the type and frequency of testing, are documented, approved, and effectively implemented.
- The frequency and rigor with which individual controls are tested depend on the risks that will be posed if the controls are not operating effectively.

Maturity Level 5 → Integration

- Effective implementation of compliance controls is second nature.
- Policies, procedures, implementations, and tests are continually reviewed and improvements are made.
- A comprehensive compliance program is an integral part of the culture.
- Decision-making is based on cost, risk and mission impact
- The consideration of compliance is pervasive in the culture
- There is an active enterprise-wide compliance program that achieves cost-effective compliance.
- Compliance is an integrated practice
- Compliance vulnerabilities are understood and managed.
- Threats are continually reevaluated and controls adapted to changing compliance environment.
- Additional or more cost-effective compliance alternatives are identified as the need arises.
- Costs and benefits of compliance are measured as precisely as practicable.
- Status metrics for the compliance program are established and met.

Annual Compliance Program Rating*

Rate the elements below on a 1-5 scale: 1 means the element does not yet exist or it exists, but at an immature, ineffective and/ or inconsistent level; 5 means the element exists and operates at a high level and is regularly assessed for effectiveness.

Element of Compliance Program	Rating
1. Top management recognizes the importance of an effective compliance program and has made it a priority company-wide.	_____
2. Members of the workforce have had some form of training or awareness in compliance topics.	_____
3. A list or matrix has been developed of all the requirements of law, clients, etc., by which our organization is bound.	_____
4. Compliance has been measured against the requirements list and gaps or deficiencies have been identified.	_____
5. Gaps or deficiencies have been prioritized and action plans have been developed to correct or safeguard against them.	_____
6. All compliance policies and procedures are documented.	_____
7. All policies and procedures are consistent with one another.	_____
8. Each member of the workforce has copies of the current policies and procedures and has been trained on them.	_____
9. All compliance policies and procedures are documented.	_____
10. All policies and procedures are consistent with one another.	_____
11. Each member of the workforce has copies of the current policies and procedures and has been trained on them.	_____
12. We require all our vendors to have responsible compliance practices.	_____
13. We have reliable methods for management to stay updated on compliance developments – legal as well as client requirements.	_____
14. One or more individuals have been assigned responsibility to manage the compliance program and every member of our workforce knows who that individual is.	_____
15. Procedures are reviewed and updated at least once pa year or sooner if laws or client expectations change.	_____
16. Provide current industry or other informational resources for employees as part of an ongoing compliance awareness program.	_____
17. Monitor performance of all employees relative to compliance.	_____
18. Establish and cultivate an information and resource relationship with an association or professional organization.	_____
19. Provide a comprehensive information privacy and compliance training program for new employees.	_____
20. Provide and support ongoing awareness compliance training for all staff.	_____
21. Outline clear expectations of each individual's professional responsibility to maintain compliance.	_____
22. Compliance breaches or incidents are documented, investigated and trended	_____

*The template for this rating system was presented during a compliance workshop conducted by the Association of Credit and Collection Professionals (ACA International).