



HIPAA

Case Study Investigation (CSI)

Baxter Healthcare Corporation

Heather L. Humphrey, CIPP
Julianne Williams
Jennie Orrico

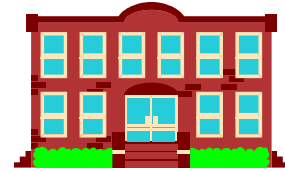
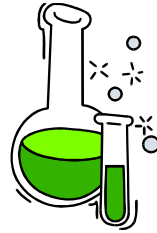


Agenda

- ❖ **HIPAA Applied to Baxter**
- ❖ **The Problem**
- ❖ **The Solution**
- ❖ **“The Survey Says...”**
- ❖ **Implications**
 - **Baxter**
 - **Business Associates**
 - **Healthcare**

The U.S. HIPAA Regulations Apply Directly to:

Health Care Providers



**Health Plans
(including self-insured
employer plans) and**



Health Care Clearinghouses





Baxter As Hybrid Entity

Hybrid Entity is defined as a single entity:

- **That is a covered entity**
- **Whose business activities include both covered and non-covered functions; and**
- **That designates its covered health care components (so that the entire organization is not a covered entity).**



Examples of Business Associate (BA) Components within Baxter

- ❖ **Baxter Healthcare – Renal Division**
 - 600 BA relationships
 - **Relationships with Renal treatment facilities**
- ❖ **Baxter Healthcare Corporation – Canadian Entity**
 - **Approximately 10 BA relationships**
 - **Assists healthcare providers deliver services through Baxter Patient Care System**

The Problem - Scope

- ❖ **Technical team contacted to implement the database replacement**
- ❖ **Focus was on U.S. Renal treatment centers**
- ❖ **Technical team contacted Baxter's Global Privacy Practices**
- ❖ **Unsure, according to HIPAA, how to meet security requirements consistent with Healthcare, Treatment and Operations during database swap**
- ❖ **We couldn't look to the BAA or to HIPAA regulation for specific procedures.**



The Solution

- ❖ **Develop a 5-question survey to identify requirements for database swap**
- ❖ **The survey would ask questions related to:**
 - **Transferring**
 - **Handling**
 - **Deleting**
 - **Storing**
 - **Assuring integrity of PHI**



The Solution (cont'd)

- ❖ **Ask the treatment centers “What do you require?”**
- ❖ **When requirements are in hand, create a “Task Guide” to be used by Technical Support Representatives (TSRs) to implement the database replacement.**



“The Survey Says...”

❖ See Handout

➤ Database Handling Customer HIPAA Survey

Implementation

- ❖ **Baxter's technical coordinator was tasked to develop and implement customer survey**
- ❖ **Randomly selected 37 treatment centers to potentially complete survey**
 - **Fairly large to smaller sized centers**
- ❖ **Vision: 20 completed surveys**
- ❖ **Baxter's technical coordinator contacted each identified center to reach out to the privacy and/or security representative**



Outcomes – General

❖ Very labor intensive

- On average it took 5 phone calls to identify the appropriate HIPAA representative;
- Approximately 156 outbound calls to 37 centers to successfully complete 20 surveys;
- 11 centers requested survey be e-mailed; 6 of these were completed and returned; and
- One customer requested the survey to be faxed. This survey was never returned.



Outcomes – Survey Specific *Question 1*

❖ Question 1:

- Which would be acceptable ways for Baxter to meet your privacy and security requirements when transferring databases containing PHI?

❖ Common Answer:

- **Use of a Secure FTP**



Outcomes – Survey Specific Question 2

❖ Question 2:

- Which of the following would be acceptable ways for Baxter to destroy PHI?

❖ Common Answer(s):

- Delete information from Baxter TSR's computer and empty the wastebasket.
- Sending any CD ROM's with PHI back to the clinic to destroy.



Outcomes – Survey Specific Question 3

❖ Question 3:

- Which would be an acceptable way to verify the integrity of the data?

❖ Common Answer:

- Have a knowledgeable person review the data before it is transmitted to Baxter and once again when the data is returned to the facility. This person would then sign a confirmation that the data has not changed.



Outcomes – Survey Specific Question 4

❖ Question 4:

- When working with the Clinic's database, if a corrupt patient record is found and needs to be deleted, hence changing the database, which of the following would be acceptable?

❖ Common Answer:

- **Baxter TSR calls the clinic to discuss, then continues support.**



Outcomes – Survey Specific Question 5

❖ Question 5:

- What type of information should be kept in a log/checklist that monitors what has transpired since the database was sent to Baxter? (Select as many options that may apply).

❖ Common Answer:

- All 20 of the individuals surveyed chose A, B, C, D, E, F, plus several individuals would like the log to include an audit of all Baxter personal who touched the data.



Implications - Baxter

- ❖ **We believe we did the proactive and right thing**
- ❖ **We have:**
 - **A HIPAA-enabling solution for our current database replacement**
 - **Documented protocol/methodology to conduct future data replacements**
 - **Working Business Associate relationships**
- ❖ **The methodology may require re-validation depending on project type**

Implications – Business Associates

- ❖ **Legal vagueness = implementation confusion**
- ❖ **What worked for Baxter's CEs may not apply to other BA's CEs**
- ❖ **Generally, discover your CEs**
 - **Who are the primary privacy and security contacts?**
 - **What are their security standards/preferences?**
 - **Do you know their data communication preferences?**
 - **What do you they expect from you?**



Implications – Healthcare

- ❖ **Legal vagueness = implementation confusion**
- ❖ **Know your requirements**
 - **What are your security standards?**
 - **Do you know your data communication preferences?**
 - **What do you expect from your Business Associates?**



Implications – Healthcare (cont'd)

- ❖ **Know and communicate widely your privacy and/or security officer**
 - **Does your receptionist know who you are?**
- ❖ **Partner with Business Associates seeking to enable covered entities HIPAA compliance**
 - **Do you view Business Associates as partners?**

QUESTIONS / ANSWERS





THE END

