Your Personalized Road Trip to HIPAA/HITECH Compliance Land

- Map your trip
- Do your maintenance
- See the sites

> Erika Bol
Privacy Officer Colorado Dept. of Health Care Policy & Financing

> Shallie Bryant
HIPAA Privacy & Security Officer, CarolMont Health

> Stephanie Helline
Owner & Creative Director, Strategic Design Studio

BE READY TO NAVIGATE THE TWISTS AND TURNS TO COMPLY WITH HIPAA/HITECH

> Erika Bol
Privacy Officer Colorado Dept. of Health Care Policy & Financing
Let’s Face It…

- HIPAA is complex
- HITECH added complexity
- New Penalty Structure & Enforcement Actions make it critical to Get It Right

"Firsts" Under HITECH

- Civil Money Penalty (CMP) of $4.3 M against Cignet health in Maryland
- Settlement with a Physician Practice (Phoenix Cardiac Surgery)
- Settlement with an Entity who reported a breach during the ‘non-compliance’ grace period
- Random, funded Audits!
Omnibus Twists… BAs

- Definition of business associate
  - Now 482 words up from 314 in HIPAA (50% increase)
  - Inclusion of many entities as per HITECH law
    - Subcontractor BAs
    - PSOs, HIOs, E-prescribing gateways, PHR vendors, entities that manage exchange of PHI through a network, entities that have access to PHI on routine basis, etc.
  - Exclusions added to definition and/or clarified
    - Treatment
    - Researcher by virtue of his/her research activities
    - Conduit exception for courier services (paper & electronic)

> Erika Bol
Privacy Officer Colorado Dept. of Health Care Policy & Financing

And Turns… Breaches

- We must now assume that an inappropriate use or disclosure of PHI is a breach
  - No longer consider “harm to patient” in assessment of whether to report or not
  - New 4-pronged test must prove “low probability of compromise of PHI” in order to NOT notify clients and federal government (& media if >500 clients)

- What does that mean for Compliance/Privacy Officers?
  - More reportable breaches to OCR (?)
  - Potential for more investigations

> Erika Bol
Privacy Officer Colorado Dept. of Health Care Policy & Financing
Omnibus Pot Hole(s)…

• Willful Neglect
  – Subjects an entity to mandatory fines and/or settlements
  – A “ticket” to a private lawsuit

• From September 2009 through end of 2012:
  – OCR received 77,200 HIPAA complaints
  – Investigated 27,500 cases
  – Issued 18,600 corrective actions, and
  – Collected $14.9 million in fines and resolution settlements

> Erika Bol
Privacy Officer Colorado Dept. of Health Care Policy & Financing

---

Omnibus Pot Hole(s)…

<table>
<thead>
<tr>
<th>Violation Category</th>
<th>Each violation</th>
<th>All such violations of identical provision in Calendar Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Did Not Know</td>
<td>$100 - $50,000</td>
<td>$1.5M</td>
</tr>
<tr>
<td>Reasonable Cause</td>
<td>$1000 - $50,000</td>
<td>$1.5M</td>
</tr>
<tr>
<td>Willful Neglect – Corrected</td>
<td>$10,000 - $50,000</td>
<td>$1.5M</td>
</tr>
<tr>
<td>Willful Neglect – Not Corrected</td>
<td>$50,000</td>
<td>$1.5M</td>
</tr>
</tbody>
</table>

> Erika Bol
Privacy Officer Colorado Dept. of Health Care Policy & Financing
Omnibus Blind Curves…

• Liability for Breaches under State and other Law
  – Curry v. AvMed Inc. (health plan in FL)
  – Court found “plausible injury” from breach
    • Case “fairly clearly” outlines what the Court views as the minimum requirements to establish causation in a data breach/identity theft case

> Erika Bol
Privacy Officer Colorado Dept. of Health Care Policy & Financing

Omnibus – Crosswalk Ahead!

• Definition of PHI limited to health information pertaining to individuals currently alive or dead less than 50 years

• May now share decedent’s PHI with family member, close friend or other individual involved in individual’s treatment or payment before his/her death (new 164.510(b) exception)

> Erika Bol
Privacy Officer Colorado Dept. of Health Care Policy & Financing
Omnibus Yield

- Business Associate Compliance
  - Now civilly and criminally liable for violations of Privacy (portions) and Security (all) Rules

- What does that mean for you as a Covered Entity?
  - More Oversight?
  - Less oversight because your BAs have it covered?

Omnibus – Backup...
Marketing

3 Pronged-test

Must meet all 3 to be marketing

1. Is it a communication that encourages an individual to purchase or use a third party’s product or service?

2. Do you receive payment (financial remuneration) from the 3rd party for making the communication?

3. Are you certain that an exception DOES NOT APPLY?
Omnibus – Backup…
Marketing (cont.)

Five (5) Exceptions:

1. Communication promotes health in general – i.e., encouraging annual mammograms
2. Communication is face-to-face - health care operations or treatment ("or other marketing communication")
3. The communication is a promotional gift of nominal value provided by the CE
4. The communication is related to refill reminders about a drug that is currently prescribed and any payment is reasonably related to the cost of making the communication
5. Is about government and government-sponsored programs (as there is no commercial component to these communications)

> Erika Bol
Privacy Officer Colorado Dept. of Health Care Policy & Financing

Marketing vs. Sale of PHI

Marketing
- For communication
- Financial remuneration
- Valid authorization required
- General statement in NPP*
- No opt out statement required in NPP
- Exceptions:
  - Face-to-face
  - Gift of nominal value
  - Refill reminders
  - General health communication
  - Government programs

Sale of PHI
- For anything
- Remuneration (of any kind)
- Valid authorization required
- General statement in NPP*
- No opt out statement required in NPP
- Exceptions
  - Treatment & payment
  - Public health
  - Transfer, merger, etc.
  - Required by law
  - To BAs
  - Research (restricted)
  - To the individual (restricted)
  - To cover cost to prepare & transmit PHI

> Erika Bol
Privacy Officer Colorado Dept. of Health Care Policy & Financing
Omnibus

• Cyber Crime is FBI’s “Nation’s Top Threat”
  – Replaced terrorism in 2012

• Medical information has street value of $50/person vs. social security # of $1/person*

• All this in an era of increased data sharing to improve quality & decrease costs

*Nationwide Insurance Chief Privacy Officer, 2012

>Erika Bol
Privacy Officer Colorado Dept. of Health Care Policy & Financing

Omnibus – U-Turn...

We simply must do better than this for our patients!

> Erika Bol
Privacy Officer Colorado Dept. of Health Care Policy & Financing

A large number of medical documents and files containing private information including Social Security numbers, addresses, dates of birth, bank account information and private health information were found in a dumpster outside of an office complex in Hiram, Ga.
Omnibus – Get Up To Speed!

Resources

Federal Register for the Final Omnibus Rule
https://www.federalregister.gov/

Office for Civil Rights
www.hhs.gov/ocr/

Office of National Coordinator
www.healthit.gov

For policies and procedures
The Privacy / Data Protection Project web site of the University of Miami School of Medicine
http://privacy.med.miami.edu/index.htm

Do Your Maintenance
don’t wait to break down on the side of the road. Move towards proactive compliance and build a culture of privacy and confidentiality.

> Erika Bol
Privacy Officer Colorado Dept. of Health Care Policy & Financing

> Shallie Bryant
HIPAA Privacy & Security Officer, CaroMont Health
About CaroMont Health

• We are a nationally recognized leader and valued partner in promoting individual health and vibrant communities
  – 3,800 employees
  – 452 medical staff
  – 268 volunteers
• Gaston Memorial Hospital, 435 beds
• CaroMont Medical Group, a network of 45 primary & specialty physician offices in 5 counties and 2 states
• Courtland Terrace, 96 bed skilled nursing facility
• Gaston Hospice

> Shallie Bryant
HIPAA Privacy & Security Officer, CaroMont Health

Proactive vs. Reactive

• What is your current environment?
• Understand the organizational workflow
  – Employee responsibility
  – Framework of system

• Understand what types of activity to monitor
  – Fire drill vs. the real thing
    – Policies & procedures?
    – NOPP?
    – Inappropriate access – snooping?

> Shallie Bryant
HIPAA Privacy & Security Officer, CaroMont Health
## Privacy Program - Structure

<table>
<thead>
<tr>
<th>Compliance Program Structure</th>
<th>Privacy Program Structure</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Standards &amp; Policies</td>
<td>• Policies &amp; Procedures</td>
</tr>
<tr>
<td>• Training &amp; Education</td>
<td>• Process to Receive</td>
</tr>
<tr>
<td>• Auditing &amp; Monitoring</td>
<td>Complaints</td>
</tr>
<tr>
<td>• Reporting</td>
<td>• Mitigation of Harmful</td>
</tr>
<tr>
<td>• Response &amp; Prevention</td>
<td>Effects</td>
</tr>
<tr>
<td>• Enforcement &amp; Discipline</td>
<td>• Safeguards to Protect</td>
</tr>
<tr>
<td>• Compliance Officer</td>
<td>Privacy</td>
</tr>
<tr>
<td></td>
<td>• Training &amp; Education</td>
</tr>
<tr>
<td></td>
<td>– Training Workforce</td>
</tr>
</tbody>
</table>

> Shallie Bryant  
HIPAA Privacy & Security Officer, CaroMont Health

## Key Points

• How is your organization identified under HIPAA?

• CaroMont Health = Affiliated Covered Entity  
  – Single Notice of Privacy Practices  
  – Centralized Governance Structure  
  • Standard  
    – Training & education  
    – Investigation & response  
    – Disciplinary actions consistent across the organization

> Shallie Bryant  
HIPAA Privacy & Security Officer, CaroMont Health
Strengths

Buy-in from Senior Leadership

AVP  EVP/General Counsel  CEO  Board of Directors

Benchmark Past Reports

2011

47.1%
7.1%
6.4%
5.0%
4.6%

2012

46.0%
8.7%
5.6%
5.6%
4.3%

> Shallice Bryant
HIPAA Privacy & Security Officer, CaroMont Health

Disclosure of Confidential Health Information - HIPAA
Unfair Employment Practices
Disclosure of Confidential Information
Guidance Request
Other

Disclosure of Confidential Health Information - HIPAA
Inappropriate Behavior
Billing and Coding Issues
Patient Care
Disclosure of Confidential Information
Weaknesses

• Limited Staff

• Absence of Privacy Culture

• Lack of Privacy Program Infrastructure

• No sense of Privacy – Multiple Areas of Risk
  – Small town (everybody is a family member or friend)

Opportunities

• Intranet Platform

• Changing Enforcement Landscape

• Training and Education
  – Lunch & Learns
  – Newsletter (HIP TIPs)
  – Corporate Compliance and Ethics Week
  – Privacy Champions
Opportunities (cont.)

Top OCR Privacy Issues
- Impermissible uses & disclosures
- Lack of safeguards
- Failure to provide access to individual
- Use & disclosure of more than minimum necessary
- Failure to provide NOPP

Top CaroMont Privacy Issues
- Impermissible uses & disclosures
  - Fax, mail, voicemail containing PHI disclosed to the wrong patients
- Snooping
  - Lack of safeguards

Potential Threats

- Privacy & Security violations getting more media attention
  - Local newspaper across the street from hospital
- Erosion of patient trust and reputational harm
- Budget constraints
  - Do more with less!

- Enforcement Landscape
  - The Omnibus HIPAA HITECH Final Rule
  - $50,000 HIPAA Breach settlement involving less than 500 patients
  - Provider settles HIPAA case for $1.5 million for potential violation
Primary Analysis

- Assessment of our privacy compliance program at CaroMont Health revealed:
  1. More focus needed to be placed on education and awareness
     - Who to contact for privacy issues/guidance
  2. HIPAA privacy policies
     - Revise our NOPP
  3. Occurrence reporting
  4. Proactive clinical system auditing & monitoring

Practical Tips for Building a Culture of Privacy
**Education & Awareness Initiatives**

- Education, training, and awareness are essential to an effective compliance program
- We have created an organization-wide, systematic approach that includes:
  - Compliance training at general corporate orientation
  - Dedicated intranet page
  - Two articles in our monthly PR/Marketing publication
  - Celebration of corporate compliance & ethics week

---

**Awareness Initiatives - Orientation**

- Opportunity to discuss compliance with all new workforce members including:
  - Employees
  - Providers
  - Volunteers
  - Students

- This venue allows for instruction directly from corporate responsibility department staff

---

> Shallie Bryant

HIPAA Privacy & Security Officer, CaroMont Health
Awareness Initiatives - Orientation

- The presentation includes information about the:
  - Corporate responsibility program at CaroMont Health
  - HIPAA/Privacy
  - Social media guidelines
  - Compliance scenarios/video clips
  - Q & A's
  - Compliance Babies

Different Methods for Delivering Messages

Celebration of Corporate Compliance & Ethics Week
"Are you Smarter than a Privacy Expert?"
Display Board game where each player selected their questions off the display board and had to answer the privacy scenarios
Education & Training

- CBLs - Computer-Based Modules
- Be visible
- In person training
  - Created to meet the need of employees (what they need to know to do their jobs)
- Newsletters
- HIPAA privacy & security basics
  - Who Xs two
  - Snooping guideline
  - Social media usage

> Shallie Bryant
HIPAA Privacy & Security Officer, CaroMont Health

Newsletter – CaroMont Connections
Policies

- Create? Revise? Update?
  Policies that follow industry standards and fit the need of your organization, big or small.
  - Code of Conduct
  - Breach Notification Policy
  - Notice of Privacy Practices Requirements
  - User Confidentiality Agreement
  - Taking Photographs and Making Recording/Audio of Patients
  - Protecting PHI of High-Profile Patients

> Shallie Bryant
HIPAA Privacy & Security Officer, CaroMont Health

Policies – Enforcement and Discipline (cont.)

- We worked with our human resources department to revise our disciplinary actions policy in an effort to provide a guideline for consistency with discipline/sanctions.

> Shallie Bryant
HIPAA Privacy & Security Officer, CaroMont Health
Hotline - Occurrence Reporting

- Hotline Awareness
  - Promote your hotline
- Tracking Trends
- Response & Prevention
  - Timely response to reported allegations
  - What to do when a breach occurs

OCCURRENCE REPORTING AND RESOLUTION
Voluntary / Anonymous

- Hotline
- Occurrence Reporting System
- Patient Private Action

- Risk Analysis and Prioritization
- Tracking & Trending
- Appropriate Response & Resolution
- Future occurrence prevention

> Shallie Bryant
HIPAA Privacy & Security Officer, CaroMont Health

So Why A Hotline?

- 24/7 Coverage
- Confidentiality
- Anonymous reporting
- Use your hotline to determine what areas need the most work
  - Employees accessing their own information
  - Snooping

It only takes ONE!
ONE number to dial, ONE person to call, ONE call to make a difference!

CaroMont Health employees are expected to provide exceptional service to our customers. This is what it means to SHINE. As part of CaroMont Health’s commitment to Corporate Responsibility, employees are encouraged to call with questions or concerns related to:

Compliance · Financial Management · Human Resources · Privacy

Feel free to call anonymously to voice your concern or ask a question relating to an issue that is inconsistent with our values and policies. Your privacy is guaranteed. Retaliation against persons reporting concerns is strictly prohibited.

1-877-785-0001
CaroMont Health Corporate Responsibility Hotline
24 hours a day, 7 days a week • Calls are confidential

shine on
Auditing & Monitoring

- Work with IS/IT to identify applications and systems to audit
- Regularly review records of information system activity

1. Understand what type of activity to monitor
   - Departments showing the highest # of incidents

Auditing & Monitoring of Clinical Systems

- **Past:** Initially we worked with IS/IT department to investigate reported issues
- **Present:** Proactive approach to monitor clinical systems to help identify users who are engaging in inappropriate patient access patterns
- **Future Goals:** To continue proactively monitoring system activity with the expectation that all inappropriate usage of our clinical systems will stop
Auditing & Monitoring of Clinical Systems
(Understanding the flow of things...)

- Monthly proactive audits are investigated, documented, and reported up to the CEO and Corporate Responsibility Committee of the Board
- Sanctions as required
- This allows us to monitor and audit trends/patterns of:
  - Suspicious Activity
  - Self Examination
  - Snooping
  - Employee/Patient Audit Alerts

In Conclusion

- Be positive
- Know your audience
- Develop a strategy
- Utilize every communication channel available to you
- Whatever your messages are, repeat them and use variety in how you spread the message

> Shallie Bryant
HIPAA Privacy & Security Officer, CaroMont Health
Top 5 Silly Privacy Questions

- Is it HIPPA or HIPAA?
- What is the Notice of Privacy Practices?
- Can a tattoo be considered PHI?
- What is PHI?
- Ativan or Xanax?

How to communicate a complex message and still have fun!

 Disclaimer:
I’m a communicator, not a privacy and compliance expert.
4 things to think about with every message you communicate

1. Audience
   • Who is it?
   • What is their level of understanding?
   • Put yourself in their shoes.

2. Goal of the communication

3. Delivery method

4. Evaluation

> Stephanie Helline
Owner & Creative Director; Strategic Design Studio
4 things to think about with every message you communicate

2. Goal of the communication

• What do you want them to understand, to learn or to do?
• It's the receiver of the message who determines the success of the message.

3. Delivery method

• What is the best way to get the message out?
• What are the tools in your tool chest?
  - monthly email newsletter
  - text message
  - internal social media network
  - lunch and break room flyer
  - flat screen monitor message / poster
  - brochure
  - training

> Stephanie Helline  
Owner & Creative Director; Strategic Design Studio
4 things to think about with every message you communicate

4. Evaluation

- Build in a method to evaluate the success of the message before you send it out.
- Your data will tell you what is working and what is not. It will help you make your case.

Let’s get our hands dirty, roll up our sleeves …

How do you explain what is a breach?

Who is the audience?
Let’s get our hands dirty, roll up our sleeves ...

The audience is

- front desk staff
- nurses
- doctors
- technicians
- executives
- everyone in your health system or practice

All with different levels of understanding.

> Stephanie Helline
Owner & Creative Director; Strategic Design Studio

What do audience members have in common?

They are:

- Busy;
- under pressure; and
- they need to learn and learn quickly.

> Stephanie Helline
Owner & Creative Director; Strategic Design Studio
What else do they have in common?

They don’t read well.

The cold hard facts

- 4 out of 10 Americans have basic or poor prose skills.
  Latest study by the Dept. of Education, adult literacy test

- If you write your message at the 11th grade level, 97% of American adults will not be able to

3 reasons you should check the readability

1. Increase your chance of reaching your readers

1. Improve communication

1. Boost the bottom line, you can
   save money
   save time
   move people to act

> Stephanie Helline
Owner & Creative Director, Strategic Design Studio
Simple messaging can save money

Joseph Kimble, author of *Writing for Dollars, Writing to Sell*, documents a case study in his book about FedEx

- FedEx: rewrote their operations manual and saved $400K a year
- How did they save the money? It took their employees less time to find the correct answer and they didn’t make as many mistakes.

---

The key to writing readable content

Pay attention to

- sentence length
- word length

Remember

- chunk it down
How short is short

It's short
• Wall Street Journal target: 5 characters per word

Remember
• Syllables: use two syllable words or less
• Sentence length: 14 words or less is best, no longer than 21 words
• Paragraphs: average 42 words per paragraph

Now I have to count characters and syllables?

It's not as complicated as it sounds.
• Free online readability tool: http://storytoolz.com

Let's see how we did with our What is a breach? brochure.

1. We started with the law.

What is a breach?
The law defines a breach as the unauthorized acquisition, access, use, or disclosure of unsecured protected health information (PHI).

2. Then explained with simple language.
People can relate to stories

We asked, “What does this mean?”

- we gave simple answers
- we told stories

(actual copy)

- if unencrypted PHI was emailed to the wrong person outside of our network – a breach has occurred
- if paper files containing confidential information that were not shredded were found in a trash can – a breach has occurred
- if an associate snoops into a co-worker’s or neighbor’s medical record – a breach has occurred

> Stephanie Helline
Owner & Creative Director; Strategic Design Studio

storyztool.com agreed

> Stephanie Helline
Owner & Creative Director; Strategic Design Studio
Write for 9th grade reading level

5th and 6th grade reading level is ideal, but very hard to attain

This message got the hotline ringing

Characters per word: 4.76

Longest sentence: 20 words

Shortest sentence: 17 words

Flesch-Kincaid Grade Level: grade 9.1

Chunk it down.
- keep it as simple as you can
- write and edit

> Stephanie Helline
Owner & Creative Director, Strategic Design Studio
The marriage of simple content and a simple visual is the art of communication
The visual can tell the story

> Stephanie Helline
Owner & Creative Director, Strategic Design Studio

The visual can tell the story

> Stephanie Helline
Owner & Creative Director, Strategic Design Studio
You can create your look

Be consistent
  - Always use your company / practice / health system logo or name.
  - Identify your department, in the same way.
  - Figure it out once, use your “look” consistently.
  - Critical info, hotline number.

Resources
  - Marketing Communications Dept.?
    - What can they offer you? Maybe not a complete campaign, but ask for templates that you can customize.
    - Ask for brand guidelines. Be a team player.

The power of visuals

Tips to remember
  - Content-related images that capture your message are the most powerful.
  - If purchasing stock images, look for one style with a variety of images; try to be consistent.
  - Stunning, shocking, humorous works visually.
  - Photograph your own employees. People love seeing people, especially people they know!
Evaluate

Progress is power

- When you get the needle to move, when the hotline number begins to ring … you want to know why.
- Document what you’ve done.
- Build in evaluation on the front end. What is the call to action? What is the one thing you want people to do or to know?
- Utilize SurveyMonkey, be creative and give away a prize for participation.

Go out and communicate!

> Stephanie Helline
Owner & Creative Director; Strategic Design Studio

Enjoy the journey! Drop us a line.

> Erika Bol
Privacy Officer Colorado Dept. of Health Care Policy & Financing
303-666-2958
Erika.Bol@state.co.us

> Shallie Bryant
HIPAA Privacy & Security Officer, CaroMont Health
704-834-2895
BryantSJ@caromonthelath.org

> Stephanie Helline
Owner & Creative Director, Strategic Design Studio
443-315-1262
stephanie@strategicdesignstudio.com