MedEd Medical Affairs Education

BAPTIST
HEALTH CARE

2024 HIPPA

HIPAA

2024

INTEGRITY
matters

Objectives

The goal of this course is to provide you with an understanding of HIPAA's Privacy and Security Rules and our obligations to protect the privacy of patient data and the security of our systems.

Upon Completion of this Module, the participant should be able to:

1. **Discuss** with the key rules and requirements of HIPAA;
2. **List** the common threats to our cyber security; and
3. **Identify** the measures we can each take to protect our patients' privacy and our organization's
4. systems and networks.

2024 HIPAA

The HIPAA Privacy Rule

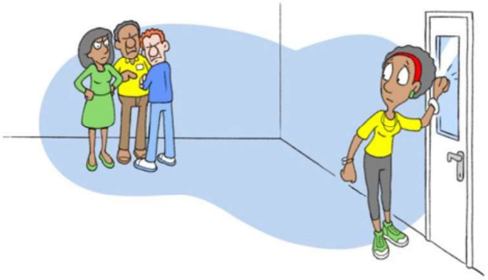
What should I do? I'm in a situation where I have to decide between reporting an action that could be damaging to Baptist Health Care or staying quiet to avoid making the situation worse. Have you ever confronted a dilemma like this? I suspect I am not alone here.

Here are the details: Recently, a local politician collapsed while giving a campaign speech and was rushed to the hospital.

In the days that followed, many news organizations started speculating as to the causes of his mysterious collapse. I work at the hospital and there is lots of buzz about his condition here as well.

Today, a fellow coworker told me she heard that several hospital employees have accessed his chart and medical records to get the real explanation for what happened to him. And they're even talking about going to the media with the information.

This leaves me wondering: should I tell someone what I know or bring it the attention of our compliance department but risk breaking the trust of my coworkers by getting involved in something that does not directly impact me?



Or should I protect myself and not say anything, but know that doing so is overlooking a breach of privacy? It's a difficult choice.

It turns out that making the right decision wasn't all that difficult, once I understood the law and Baptist's policy. I'd like to share what I discovered; in case it might help you if you ever encounter a similar situation.

This issue has to do with the federal law protecting private health information; it's called the Health Insurance Portability and Accountability Act – or "HIPAA." The first step in understanding how to deal with situations involving HIPAA is being able to DEFINE what it is.

HIPAA is a set of privacy and security regulations that prohibit access to and disclosure of Protected Health Information, or "PHI." PHI includes individually identifiable health information in any form, whether on paper, spoken or electronic.

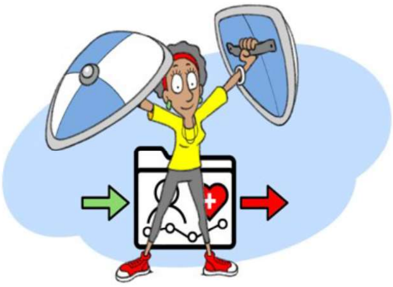
PHI also includes personal identifying information like a patient's date of birth or Social Security number.

PHI even includes the fact that a person is a patient of Baptist.

PHI may only be disclosed in certain very limited circumstances.

2024 HIPAA

So, once I understood how to define HIPAA and PHI, the next thing I had to be aware of was our responsibility for PROTECTING the personal health data that comes into our possession or is delivered to third parties.



Here are some common ways HIPAA can be violated if we are not careful:

- Losing a laptop or unencrypted flash drive;
- Faxing a lab result to the wrong physician;
- Emailing or mailing PHI to the wrong patient;
- Leaving PHI on a printer that is accessible to others without a need to see the PHI;
- Discussing a patient's care in a public space where others can overhear; or
- Disclosing to our friends/family that we saw a certain person at the hospital today.

SNOOPING is one of the most common ways our Team Members intentionally or unintentionally can violate HIPAA.

Snooping is accessing PHI without a need a know that information to do your job.

As healthcare workers, it can be tempting to access the PHI of our family, friends, neighbors, co-workers, celebrities, etc. Sometimes our friends or family may even ask you to look up their information, however **unless you must access that PHI to do your job, your actions are a violation of HIPAA and BHC policy.**

It is even considered snooping and a violation of BHC policy to **access your own PHI** outside of the formal channels like the patient portal or ROI department.

The last step is making sure that, whenever we come across a situation in which PHI may be compromised, we REPORT it immediately to the compliance office.

Getting back to the situation involving my coworkers and the medical information about the local politician, I knew that I needed to speak up because the law had been broken and the damage would very likely escalate if it wasn't addressed.

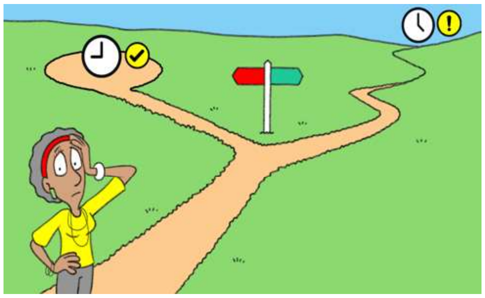
So, I reported the situation to the compliance office. They will ensure that the right steps are taken to investigate the breach of privacy and contain the exposure.

Now, I'm feeling relieved about this decision, and I hope you are too!

2024 HIPAA

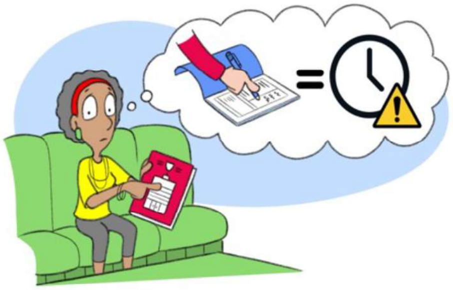
The HIPAA Security Rule

What should I do? I'm facing a situation where I have to decide between meeting a critical deadline and not following Baptist's policy. If you have ever found yourself in a similar situation, hearing about my experience might help you.



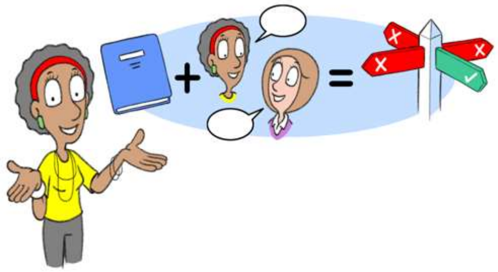
Here is my situation: I was asked to oversee the conversion of patient X-ray films to a digital format. The project is high priority, as we need to demonstrate improvements in operational efficiency by year-end.

I've identified an outside firm to perform the task, but I also know that requiring them to complete a written business associate agreement, or BAA, prior to beginning any work can mean a significant delay. And I need this project to get started as soon as possible if I have any hope of finishing it by year end.



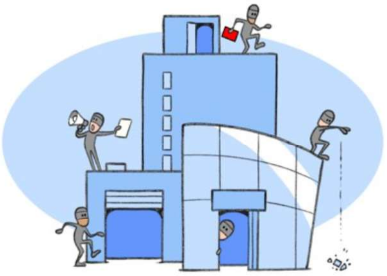
So, now I am not sure if I should proceed with the project, knowing that the business associate agreement will not be signed, so I don't get behind? Or do I refer the third-party firm to our legal department, knowing that doing so will likely cause me to fail to achieve my assigned goal?

Once I thought things through, the decision wasn't as challenging as it seemed at first. Consulting Baptist's policy again and speaking to our legal department helped me clarify the best course of action. I am hoping that you can learn from what I discovered.



The issue here concerns the *HIPAA Security Rule*. The HIPAA Security rule requires healthcare professionals to secure protected health information, or PHI, from data breaches, tampering or deletions.

Without these security measures in place, Baptist Health Care becomes vulnerable to data breaches where unauthorized people can access, modify, disclose, or even destroy valuable patient information.



Violations of this rule can lead to serious financial, legal and reputational consequences for our organization.

Once I understood the definition of HIPAA security, the next step was to BE ALERT to all possible vulnerabilities that could compromise our systems and data.

2024 HIPAA

Here are some common ways we can violate the HIPAA Security Rule if we are not careful:

- Sharing my password
- Giving out my personal information without verifying that the requestor is legitimate
- Using thumb drives or disc drives without screening the drive or disc for viruses
- Failing to update software or password resets
- Emailing PHI to my google email so I can work on a project at home
- Giving third party vendors access to our systems without a Business Associate Agreement in place

One of the biggest threats to BHC's operations is a practice known as PHISHING. Phishing is a cybercrime in which you are contacted by email, telephone, or text message by someone posing as a legitimate institution or person to lure you into providing sensitive data such as personally identifiable information, banking or credit card details, and passwords.

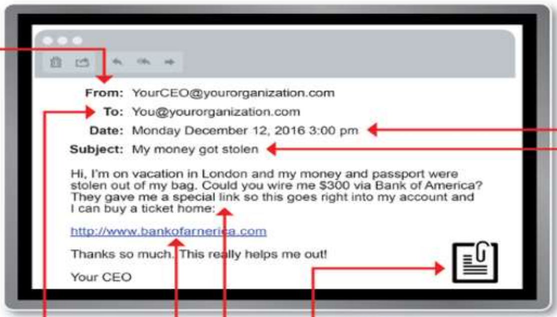
The information is then used to access important accounts or networks and can result in identity theft, financial loss, or the installation of malware / ransomware on the victim's machine or network.

If you are not sure about the legitimacy of an email you receive, notify the Baptist IT Help Desk or our Information Security team IMMEDIATELY and do not take action requested by the sender of the email.

No one inside BHC will ever request your password via email. If you see that request, report it immediately.

2024 HIPAA

Social Engineering Red Flags



From: YourCEO@yourorganization.com
To: You@yourorganization.com
Date: Monday December 12, 2016 3:00 pm
Subject: My money got stolen

Hi, I'm on vacation in London and my money and passport were stolen out of my bag. Could you wire me $300 via Bank of America? They gave me a special link so this goes right into my account and I can buy a ticket home:

http://www.bankofarnerica.com

Thanks so much. This really helps me out!

Your CEO

FROM

- I don't recognize the sender's email address as someone **I ordinarily communicate with**.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
- Is the sender's email address from a **suspicious domain** (like micorsoft-support.com)?
- **I don't know the sender personally** and they **were not vouched for** by someone I trust.
- **I don't have a business relationship** nor any past communications with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I haven't communicated with recently.

TO

- I was cc'd on an email sent to one or more people, but **I don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

HYPERLINKS

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link-to address is for a different website**. (This is a **big** red flag.)
- I received an email that only has **long hyperlinks with no further information**, and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known web site. For instance, www.bankofarnerica.com — the "m" is really two characters — "r" and "n."

DATE

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?

SUBJECT

- Did I get an email with a subject line that is **irrelevant** or **does not match** the message content?
- Is the email message a reply to something **I never sent or requested**?

ATTACHMENTS

- The sender included an email attachment that **I was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly **dangerous file type**. The only file type that is **always safe to click on is a .txt** file.

CONTENT

- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value**?
- Is the email **out of the ordinary**, or does it have **bad grammar** or **spelling errors**?
- Is the sender asking me to click a link or open up an attachment that **seems odd** or **illogical**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?

To ensure that Baptist's information stays secure and operational, we must always:

- Be alert to anyone attempting to gain access to our system or facilities. Even when our devices are locked, an experienced hacker can enter systems if they have physical access and enough time.

- Be sure to contact security immediately if you notice any person, whether it's an employee or a stranger, in any unauthorized area.

2024 HIPAA

- Lock computer, laptop, and phone screens when they are not in use.

- Use secure passwords and update them in a timely
- manner.

- Protect our passwords and badges (never share them).

- Protect our devices and never leave them unattended or in public view.

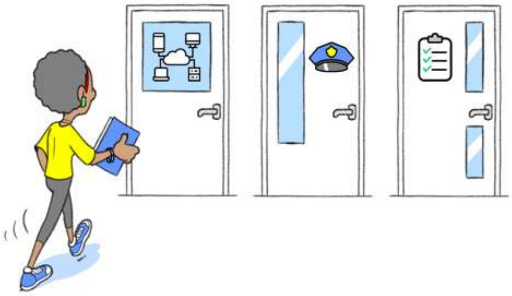
- Report instances of theft to IT immediately.

- Encrypt PHI sent by email or uploaded to the cloud.

- Use virtual private networking, or "VPN," instead of using unsecure public wi-fi.

- Never click on links, enter credentials, or provide account or user details in response to emails from unknown senders or from unexpected emails, as these can be phishing attempts.

And, of course, IMMEDIATELY report any suspected data breach to our IT or compliance departments, no matter how insignificant you think it might be.



2024 HIPAA

As you can probably tell by now, I decided **not** to start the project using the outside firm without the BAA in place. Yes, it did cause a short delay in the project and I was anxious waiting to get started, but I know I did the right thing.

And I avoided any consequences of violating our organization's policy and the law, leaving our information safe and secure.

That certainly made me feel better and I hope the information is useful for you, too!

2024 HIPAA

In closing, here are some ways we can each protect PHI and comply with the requirements of HIPAA and our policies:

- Limit access to protected health information to those who have been authorized to have that access.
- Make sure you log off your computers when not in use.
- Use only password protected electronic communications and keep company equipment with protected information in an approved, secure location.
- Never share your password.
- Never download or install applications that have not been approved by the Baptist IT department first.
- Check and double-check email addresses or fax numbers before you send any protected health information.
-
- The transmission of protected health information via email is prohibited unless authorized and performed in accordance with Baptist policies and procedures, including the requirement to encrypt any email that contains protected health information.
- Send only the protected health information necessary to fulfill the request.
-
- Before speaking with a patient or scanning records to a patient's medical record, be sure to validate that you are engaging with the correct patient.
- Report suspicious emails to the Baptist IT Help Desk IMMEDIATELY and do not take the action requested in the email.
- Do not snoop in your medical record or that of anyone else, EVER.

2024 HIPAA

If you have any questions about our HIPAA privacy, security, or other compliance issues, please contact our compliance department. We're here to help.

BHC Compliance Office	BHC Compliance Hotline
448.227.3850 compliance@bhcpns.org	704.323.4980 ebaptisthhealthcare.ethiscpoint.com

Ask Yourself:

- What feels wrong about this situation or action?
- Is this situation against Baptist policies or the law?
- How could my decision affect Baptist as a whole?
- How could my decision affect Baptist's reputation and my own?