

The Privacy and Security of Protected Health Information_2014

1. UHA_HIPAA2012

1.1 Splash



1.2 Welcome



1.3 Disclaimer

Test Your Understanding...

There's a lot to learn about our confidentiality and privacy rules. As you move through this course, we'll stop along the way and test your understanding of the topics you've just read.

Your score will determine if you need to take a separate multiple-choice test in HealthStream, following this module. So, please do your best to read each screen and answer the built-in quiz questions. Each question is worth 10 points...you'll need 80+ points to pass!

Please click the Agreement button below to confirm that you understand this information.

Agreed! I understand that I will be tested throughout the course.



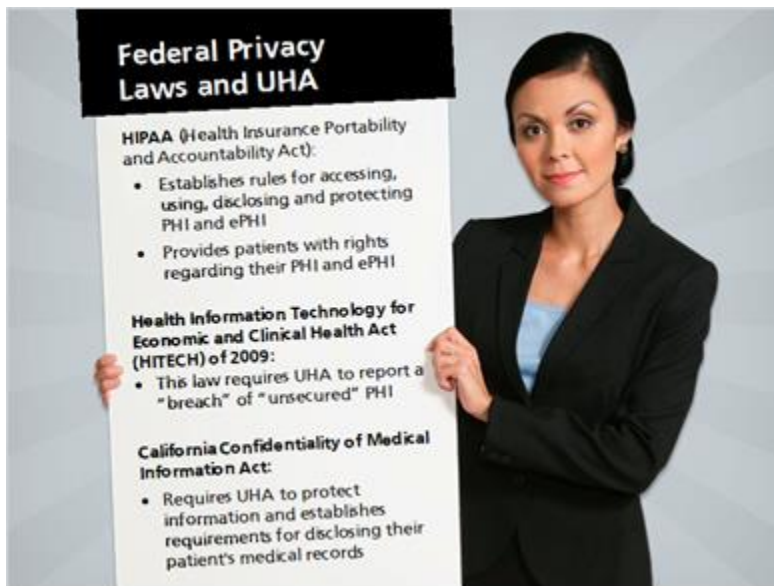
1.4 The Law

So, why do we care about **Protecting Health Information**?
Click on each information box to learn more.



- About the Law
- Federal Definition
- State Definition
- What is PHI or ePHI?

1.5 Privacy and Security Laws



1.6 Identifying PHI



1.7 Privacy Rules




1.8 Minimum Necessary

PRIVACY RULE:
Minimum Necessary

The concept of minimum necessary should be your guiding principle whenever you access, use, disclose or request PHI. Minimum necessary simply means that reasonable efforts must be made to limit the amount of PHI accessed, used, disclosed or requested in order to accomplish the intended purpose.

Violations of the "minimum necessary" principle are regarded as a security incident, which requires potential reporting.

It is important to note that the minimum necessary rule permits healthcare providers to exchange PHI as necessary to effectively treat and coordinate healthcare.

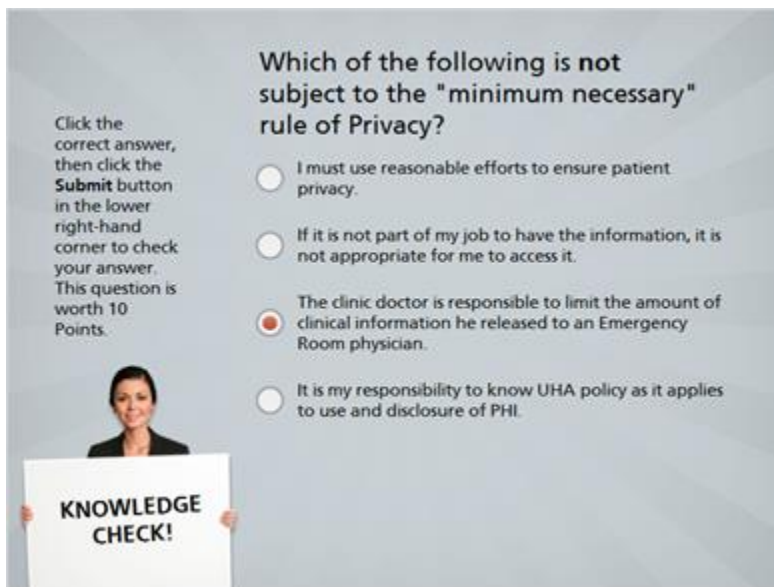
A woman with dark hair, wearing a black blazer over a blue top, stands with her hands on her hips, looking directly at the camera. She is positioned on the right side of the slide, partially overlapping the text area.

1.9 Minimum Necessary Examples



1.10 Knowledge Check

(Multiple Choice, 10 points, unlimited attempts permitted)



Correct	Choice	Feedback
	I must use reasonable efforts to ensure	That's not the correct answer. It is

	patient privacy.	important to note that the minimum necessary rule does not mean that healthcare providers should restrict the exchange of PHI to effectively treat and coordinate healthcare. Please try again.
	If it is not part of my job to have the information, it is not appropriate for me to access it.	That's not the correct answer. It is important to note that the minimum necessary rule does not mean that healthcare providers should restrict the exchange of PHI to effectively treat and coordinate healthcare. Please try again.
X	The clinic doctor is responsible to limit the amount of clinical information he released to an Emergency Room physician.	Correct! It is important to note that the minimum necessary rule does not mean that healthcare providers should restrict the exchange of PHI to effectively treat and coordinate healthcare.
	It is my responsibility to know UHA policy as it applies to use and disclosure of PHI.	That's not the correct answer. It is important to note that the minimum necessary rule does not mean that healthcare providers should restrict the exchange of PHI to effectively treat and coordinate healthcare. Please try again.

1.11 Safeguarding PHI



1.12 Safeguarding PHI Examples



1.13 Safeguarding ePHI Examples

Safeguarding ePHI: Examples and Guidelines

Here are some guidelines you should follow to keep our patients' ePHI safe:

- Do not share your password with others; use strong passwords.
- Password protect computers and cells phones.
- Turn computer monitors away from public view or use privacy screen.
- Minimize screens or lock your computer screen when you walk away from your workstations.
- Never leave portable devices with PHI, such as laptops, flash drives, and smartphones, unsecured and unattended in your car or public areas.




1.14 Incidental Disclosures

Incidental Disclosures

HIPAA recognizes that PHI may be incidentally disclosed to others when healthcare providers communicate with each other in order to provide for the appropriate and efficient treatment of patients.

These incidental disclosures are permissible so long as reasonable precautions are taken to limit what is said and who overhears the conversation.




1.15 Incidental Disclosures


Incidental Disclosures:
Examples

Here are some examples of incidental disclosures that might occur at UHA, particularly where every reasonable effort is taken to ensure patient privacy:

- Health care staff orally discussing a patient and coordinating services at a nursing station.
- Discussing lab results with a patient in a joint treatment room.
- Discussing a patient's condition with the patient on the phone.
- Calling out a patient's first or last name in a waiting room.



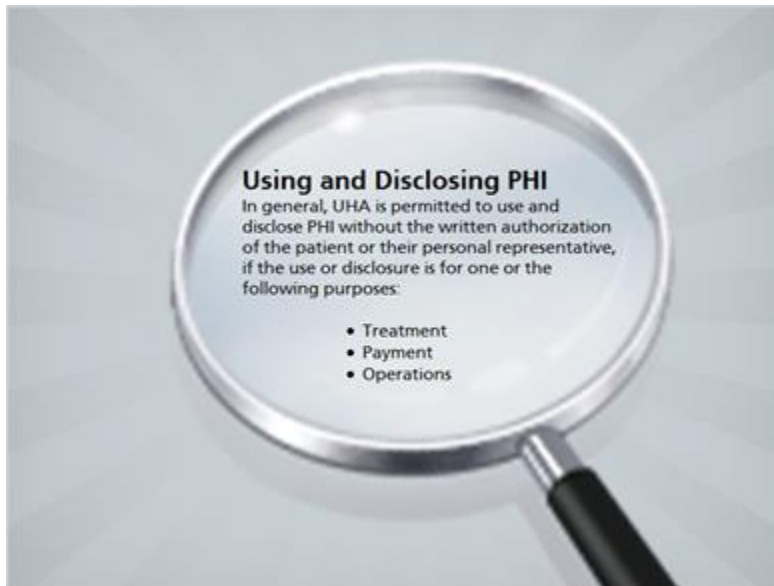
1.16 Reasonable Precautions



So, now you know more about Incidental Disclosures. Do you know what **reasonable precautions** to take to lessen the impact of incidental disclosures?
Click the button below to learn more.

Examples of Reasonable Precautions

1.17 Using and Disclosing PHI




1.18 Treatment

USING AND DISCLOSING PHI:
Treatment


Treatment means the provision, coordination or management of health care services.

Examples include:

- A patient presenting at a UHA clinic for a physical examination and laboratory tests
- A cardiologist who needs to consult with a patient's primary care physician
- A nurse practitioner who provides services at a skilled nursing facility
- A primary care physician who is coordinating care for a patient who requires home health services

A woman with dark hair, wearing a black blazer, is shown from the waist up, pointing her right hand towards the list of examples.

1.19 Payment



**USING AND DISCLOSING PHI:
Payment**

Payment refers to any activity necessary to obtain payment or to be reimbursed for health care services provided.

Examples include:

- Efforts to determine eligibility for coverage of a health care services.
- Sending PHI to a health plan so that they can determine whether they are required to pay the claim for that service.

1.20 Health Care Operations



**USING AND DISCLOSING PHI:
Health Care Operations**

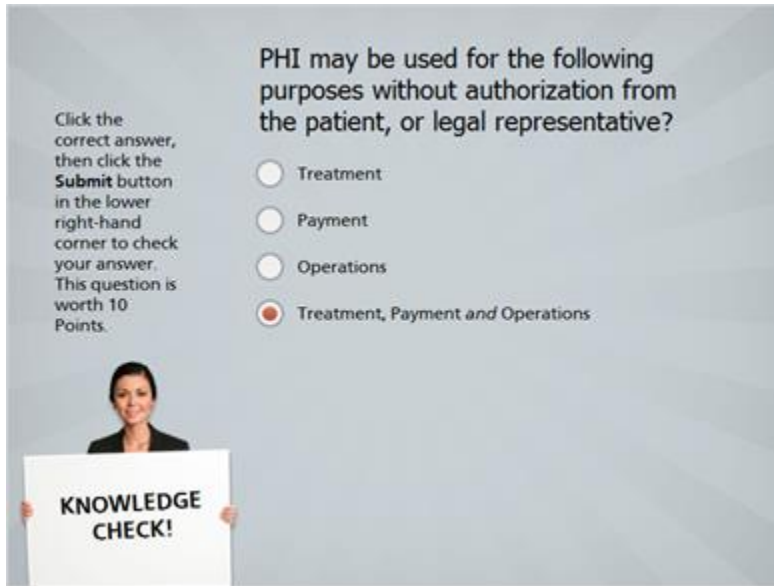
Health care operations refers to internal operational activities necessary to run UHA.

Examples include:

- Administrative activities such implementing and managing clinic schedules.
- Financial activities such as monitoring and responding to claim denials and/or governmental audit activities.
- Legal or risk management functions.
- Quality improvement activities.

1.21 Knowledge Check

(Multiple Choice, 10 points, unlimited attempts permitted)



Correct	Choice	Feedback
	Treatment	That's not the correct answer. In general, UHA is permitted to use and disclose PHI for provision/management of healthcare, in order to obtain payment for those services and to accomplish internal operations without specific patient authorization. Please try again.
	Payment	That's not the correct answer. In general, UHA is permitted to use and disclose PHI for provision/management of healthcare, in order to obtain payment for those services and to accomplish internal operations without specific patient authorization. Please try again.
	Operations	That is not the correct answer. In

		<p>general, UHA is permitted to use and disclose PHI for provision/management of healthcare, in order to obtain payment for those services and to accomplish internal operations without specific patient authorization. Please try again.</p>
X	Treatment, Payment and Operations	<p>That's Correct! In general, UHA is permitted to use and disclose PHI for provision/management of healthcare, in order to obtain payment for those services and to accomplish internal operations without specific patient authorization.</p>

1.22 Family and Friends



1.23 More About Family and Friends



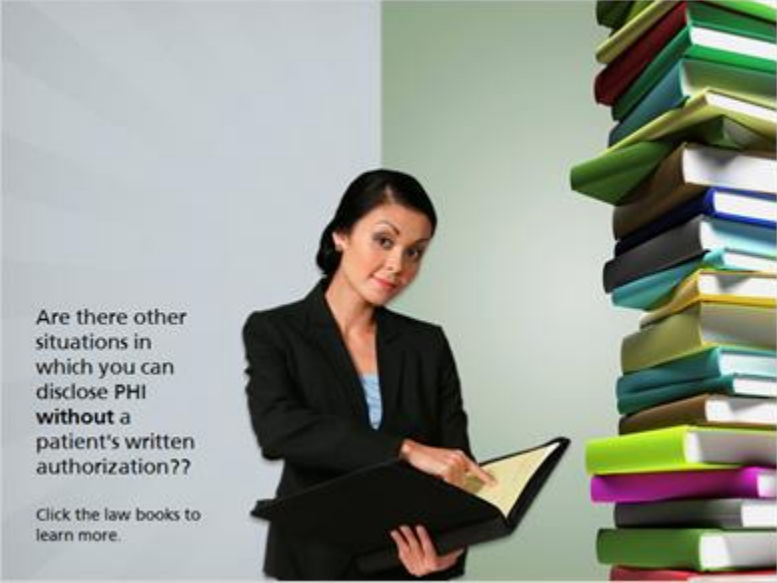
More About Families and Friends

When disclosing PHI to family and friends involved in the care of the patient, it is important to note that you should **limit** what you disclose to that which is relevant for the encounter.

Examples of permitted disclosures to family and friends, may include but are not limited to:

- Conferring with a patient's spouse about relevant past medical history.
- Discussing treatment options with a patient's significant other who attends a clinic visit.
- Instructing a patient's roommate on proper post procedure care.
- Discussing payment options with an adult patient's parents.

1.24 Authorizations



Are there other situations in which you can disclose PHI **without** a patient's written authorization??

Click the law books to learn more.

1.25 More About Authorizations



More About Authorization

Uses or disclosures of PHI for any other purpose will generally require the written authorization of the patient and/or his/her personal representative.


State and Federal law also requires a written authorization to disclose *treatment-related* PHI for these situations:

- psychotherapy
- mental health
- substance abuse
- HIV testing
- ...and other sensitive issues.

Any questions about disclosures of PHI should be directed to the UHA Director of Compliance.

1.26 Knowledge Check

(True/False, 10 points, unlimited attempts permitted)



Click the correct answer, then click the **Submit** button in the lower right-hand corner to check your answer. This question is worth 10 Points.

Some disclosures of PHI will require the patient's written authorization. True or False?

☒ True

☐ False

Correct	Choice
X	True

False

Feedback when correct:

That's right! Different situations require written authorizations, as you've just read. Questions? Talk to your supervisor or the Director of Compliance.

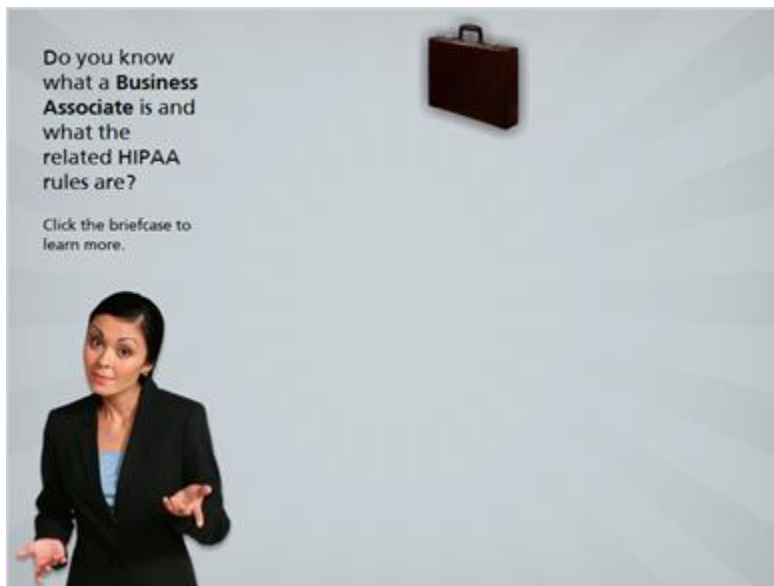
Feedback when incorrect:

You did not select the correct response. Different situations require written authorizations, as you've just read. Questions? Talk to your supervisor or the Director of Compliance. Please try again.

1.27 Verification Requirement



1.28 Business Associates



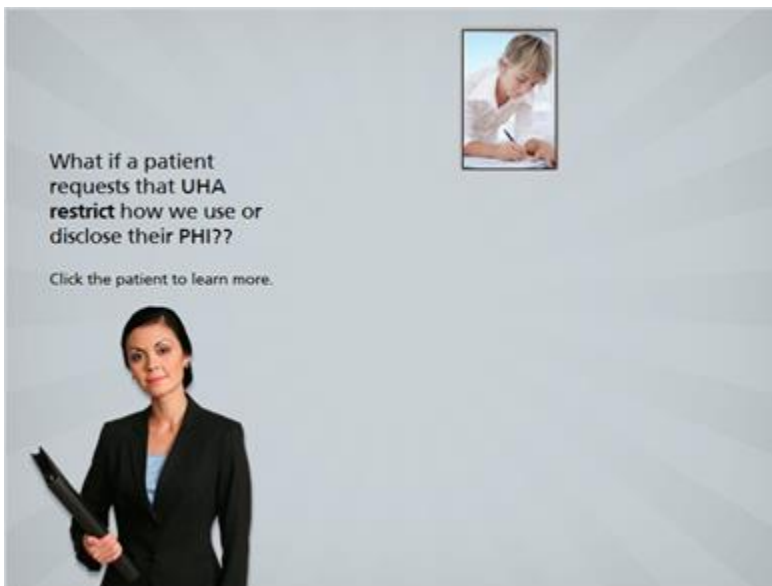
1.29 Patient Rights



1.30 Request for Confidential Communications



1.31 Requests Restrictions



1.32 Access to Medical Records



Access to Medical Records


Both HIPAA and state law permit patients or their personal representatives to have access to and to make copies of their medical and related records (e.g. billing, registration, etc.).

Under HIPAA, UHA can deny access to such records under limited circumstances and provided that specific processes are followed.

Please contact the UHA Director of Compliance or with any questions.

1.33 Knowledge Check

(Multiple Choice, 10 points, unlimited attempts permitted)



Click the correct answer, then click the **Submit** button in the lower right-hand corner to check your answer. This question is worth 10 Points.

Under HIPAA, patients do **not** have the right to?

- ☐ Request that we limit the PHI we disclose to an insurance company paying the bill.
- ☐ Request that we send billing information to a PO Box number.
- ☐ Request to review and/or copy their medical record.
- ☒ Patients have a right to all of the above.

Correct	Choice	Feedback
	Request that we limit the PHI we	That's not correct. HIPAA and state law

	disclose to an insurance company paying the bill.	permits patients, or legal representative, to access/copy medical and related records. Under HIPAA, UHA can deny access under limited circumstances, following specific processes. Try again.
	Request that we send billing information to a PO Box number.	That's not correct. HIPAA and state law permits patients, or legal representative, to access/copy medical and related records. Under HIPAA, UHA can deny access under limited circumstances, following specific processes. Try again.
	Request to review and/or copy their medical record.	That's not correct. HIPAA and state law permits patients, or legal representative, to access/copy medical and related records. Under HIPAA, UHA can deny access under limited circumstances, following specific processes. Try again.
X	Patients have a right to all of the above.	Correct! HIPAA and state law permits patients, or legal representative, to access/copy medical and related records. Under HIPAA, UHA can deny access under limited circumstances, following specific processes.

1.34 Tracking Disclosures

What are the rules for tracking HIPAA disclosures?

Click the employee to learn more.

A woman with dark hair, wearing a black blazer, is shown from the chest up. She is in a thinking pose, with her right hand near her chin. In the upper right corner of the slide, there is a small, square inset photo of the same woman, looking directly at the camera.

1.35 Corrections

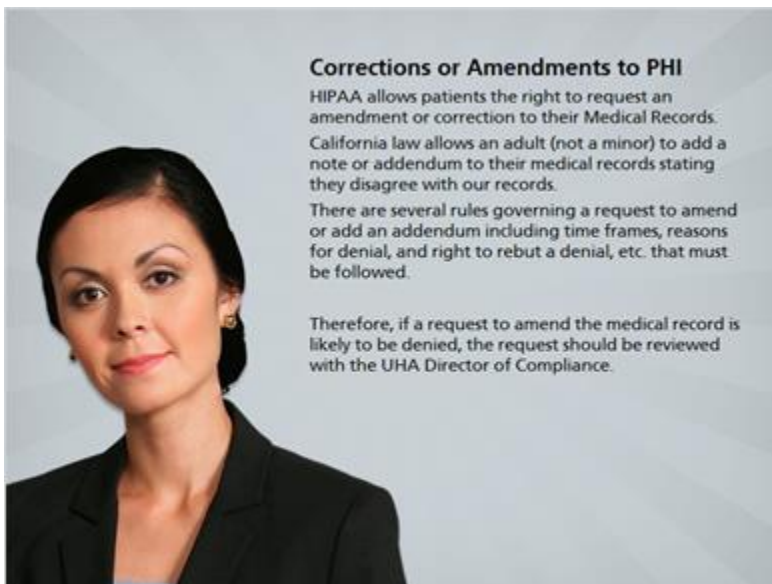
Corrections or Amendments to PHI

HIPAA allows patients the right to request an amendment or correction to their Medical Records.

California law allows an adult (not a minor) to add a note or addendum to their medical records stating they disagree with our records.

There are several rules governing a request to amend or add an addendum including time frames, reasons for denial, and right to rebut a denial, etc. that must be followed.

Therefore, if a request to amend the medical record is likely to be denied, the request should be reviewed with the UHA Director of Compliance.

A woman with dark hair, wearing a black blazer, is shown from the chest up. She is looking directly at the camera with a slight smile.

1.36 Filing a Complaint



Filing a Complaint

Patients have a right to file a complaint with UHA and/or the Office of Civil Rights if he or she believes UHA has or has the potential for violating HIPAA.

All HIPAA complaints or concerns, including those from patients, **must** be directed to the UHA Director of Compliance.

1.37 What is HIPAA Security?



What is HIPAA Security?

The HIPAA Security Rule applies to all **electronic protected health information (ePHI)** stored and/or transmitted using various forms of technology.

1.38 Examples of Technology

Where Do We Store ePHI?
Here are some examples of the technology we use to store ePHI.

- UHA Desktop PCs
- UHA Laptops
- UHA Tablets (e.g. iPads)
- UHA-issued Smartphones
- UHA Servers
- UHA Networks
- UHA Tapes
- UHA-issued USB devices
- UHA-issued Flash drives
- UHA-created CDs
- UHA-created DVDs



1.39 Workforce Expectations

As a UHA employee or contracted health care provider, what are the **expectations** for protecting ePHI?

Click the employee to learn more.



1.40 Knowledge Check

(Word Bank, 10 points, unlimited attempts permitted)

At UHA, which of these devices, with the proper security protections, **may** contain or store our patients' PHI?

Drag your answer to the space above!

Personal Smart Phones

Personal USB or Flash Drives

UHA Desktop computers

Personal home computers

Personal Portable Hard Drive

Use your mouse to **drag** the correct answer into the "answer space" just under the question, then click the **Submit** button in the lower right-hand corner to check your answer. This question is worth 10 Points.

Correct	Choice	Feedback
	Personal Smart Phones	That's not correct. Under no circumstances is it permissible to an employee to send, or maintain, PHI on personal computers, in personal e-mail account, etc. Please try again.
	Personal USB or Flash Drives	That's not correct. Under no circumstances is it permissible to an employee to send, or maintain, PHI on personal computers, in personal e-mail account, etc. Please try again.
X	UHA Desktop computers	That's correct! Under no circumstances is it permissible to an employee to send, or maintain, PHI on personal computers, in personal e-mail account, etc.
	Personal home computers	That's not correct. Under no

	<p>circumstances is it permissible to an employee to send, or maintain, PHI on personal computers, in personal e-mail account, etc. Please try again.</p>
Personal Portable Hard Drive	<p>That's not correct. Under no circumstances is it permissible to an employee to send, or maintain, PHI on personal computers, in personal e-mail account, etc. Please try again.</p>

1.41 Security Policies



1.42 Access Controls



Access Controls Policy

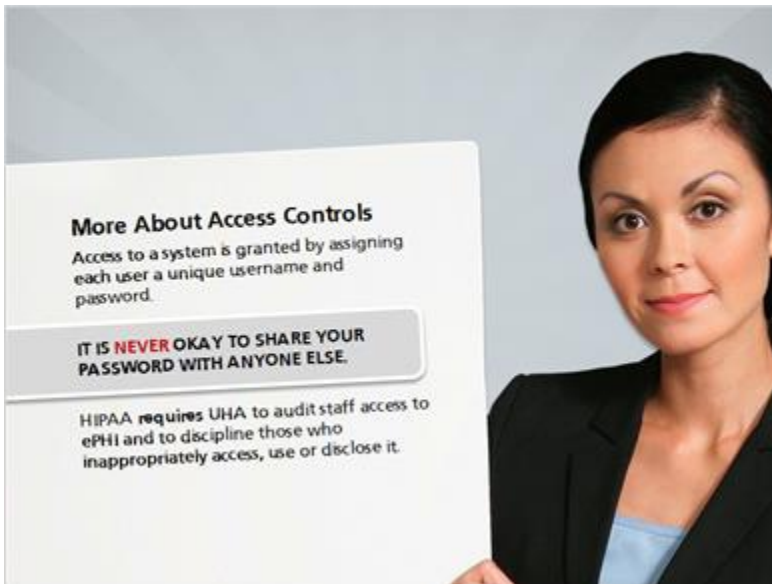
This process establishes and maintains user accounts and access rights to electronic systems, including those with ePHI (e.g. Epic).

Requests to get access to these systems are based on clinical and business needs, and will be limited to the information necessary to do your job.

Your manager determines what systems and what level of access you will be given.

Managers are required to notify UHA Human Resources whenever a member of its workforce leaves or changes roles. UHA HR will work with UHA IT to modify or terminate user's access to systems.

1.43 More About Access Controls



More About Access Controls

Access to a system is granted by assigning each user a unique username and password.

IT IS NEVER OKAY TO SHARE YOUR PASSWORD WITH ANYONE ELSE.

HIPAA requires UHA to audit staff access to ePHI and to discipline those who inappropriately access, use or disclose it.

1.44 Workstation Security



Workstation Security Policy

UHA IT will direct any installation, updates or necessary fixes to UHA computer systems. All software must be approved and installed by UHA IT.

- Only approved devices may be connected to UHA systems.
- Only UHA employees, contracted health care providers and business associates may have access to UHA computers.

ePHI should **not** be stored on a workstation-ePHI should be stored on a network server or shared drive. Workstations in public areas should be located so that information on displays are not easily viewable.

1.45 Tips for Workstation Security



Tips on Workstation Security

- Workstations are configured to turn on a screensaver after a specific amount of time
- This helps ensure that unauthorized users are unable to view ePHI
- Passwords should be "strong," which means they include letters, numbers and characters like %, !, or #
- This makes it default for others to try and use your password
- If you see someone sharing or using another co-worker's password, immediately report it to the UHA Director of Compliance


• **Never** share or request another's password or username

1.46 Acceptable Internet Use

Acceptable Internet Use: Rules and Policies

Here are some rules and policies related to Internet and e-mail use at UHA:

- UHA computers, including Web and e-mail should be used only for UHA related purposes.
- E-mails are not private and may be monitored.
- It is against UHA policy to download music, software programs, or illegal files.
- Inappropriate access to the Internet includes but is not limited to gambling and pornography.
- Internet traffic can be tracked and is monitored.
- You may **not** post identifiable patient information or photographs on social media sites such as Facebook or Twitter.



1.47 Knowledge Check


(True/False, 10 points, unlimited attempts permitted)

Click the correct answer, then click the **Submit** button in the lower right-hand corner to check your answer. This question is worth 10 Points.

If I share my office with another staff person, it is ok for me to share my password with them in case I am not here and they have to answer a question. True or False?

☐ True

☒ False



Correct	Choice
	True

X

False

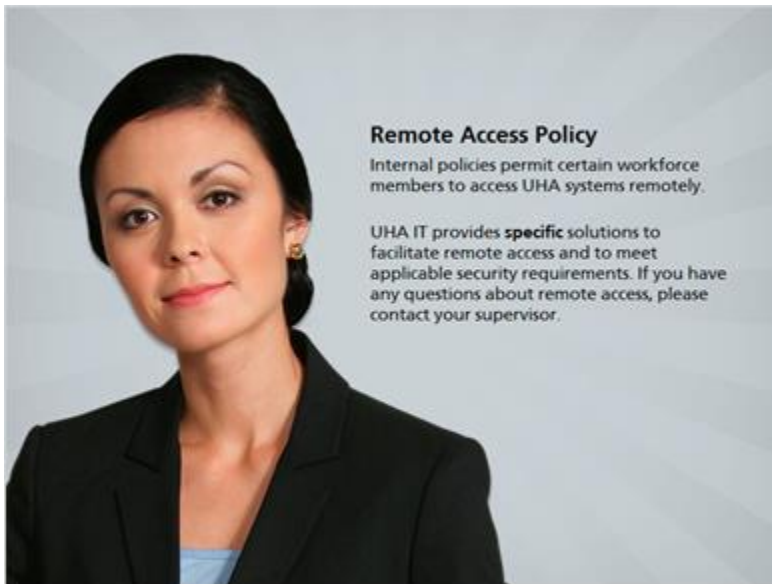
Feedback when correct:

That's right! It is never permissible to share your password. If there is a need for questions to be answered in your absence, discuss how to best accomplish this with your supervisor.

Feedback when incorrect:

You did not select the correct response. It is never permissible to share your password. If there is a need for questions to be answered in your absence, discuss how to best accomplish this with your supervisor.

1.48 Remote Access



1.49 External Communications



External Communication of ePHI Policy
All forms of external data transfer of ePHI (e.g. e-mail, file transfers or computer-to-computer exchanges) must meet specific security requirements utilizing approved solutions.

Communicating with patients:

- Raises security concerns because messages travel over un-secure public networks
- UHA is deploying MyHealth to facilitate physician-to-patient communication
- Never use non-approved solutions such as Gmail, hotmail etc.

Communicating with external health care providers:

- Must follow standardized protocols for security, reliability and manageability

1.50 e-Mail and ePHI



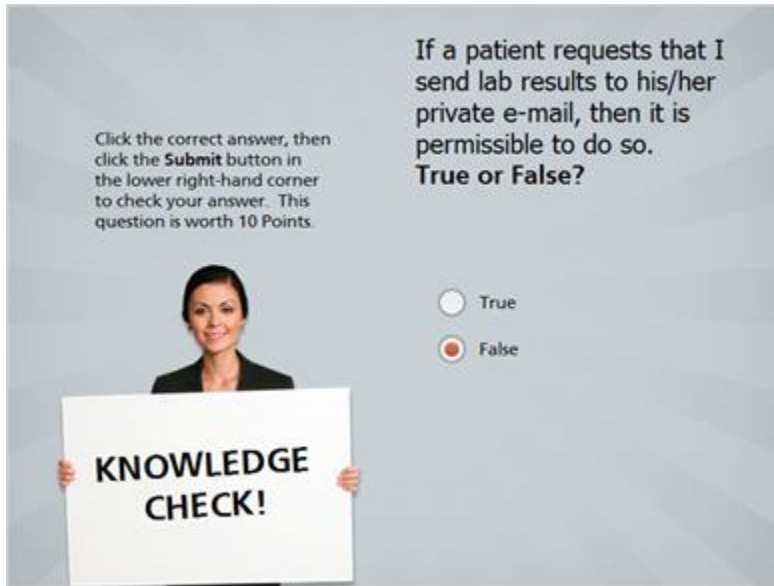
E-Mail and ePHI
All UHA employees should exercise good judgement and make reasonable efforts to use e-mail in an effective manner.

You should **not** use any e-mail system to communicate with patients. E-mail systems, including UHA-controlled e-mail systems, are not designed to serve as a means to send and receive ePHI. **Using e-mail to communicate patient information will expose UHA to the high probability of a patient privacy breach.**

If your job requires you to communicate with a patient electronically, you **must** use MyHealth to ensure that patient communication remains secure.

1.51 Knowledge Check

(True/False, 10 points, unlimited attempts permitted)



Correct	Choice
	True
X	False

Feedback when correct:

That's right! There are strict regulations that apply to the maintenance and transmission of PHI. As UHA is bound by these regulations, even with patient permission, transmission of PHI to personal devices is prohibited.

Feedback when incorrect:

You did not select the correct response. There are strict regulations that apply to the maintenance and transmission of PHI. As UHA is bound by these regulations, even with patient permission, transmission of PHI to personal devices is prohibited.

1.52 Monitoring Use



Monitoring and Appropriate Use of ePHI Policy

All access and traffic through UHA computer systems can be monitored and tracked.

UHA regularly monitors and audits computer system use, especially those with ePHI.

UHA employees and contracted health care providers who are found to be accessing or attempting to access data not necessary for their job are subject to discipline up to and including termination.

1.53 Re-Use and Disposal



Re-Use and Disposal of Computers and Media Policy

Strict security measures must be followed prior to the use, re-use and/or disposal of computer systems and portable media containing ePHI.

All data and software will be removed or destroyed using procedures that make the data unrecoverable.

Users of computers or portable devices such as laptops, smartphones, or tablets that access UHA systems containing ePHI **must** follow UHA security policies set forth for such devices, including methods for terminating UHA system access.

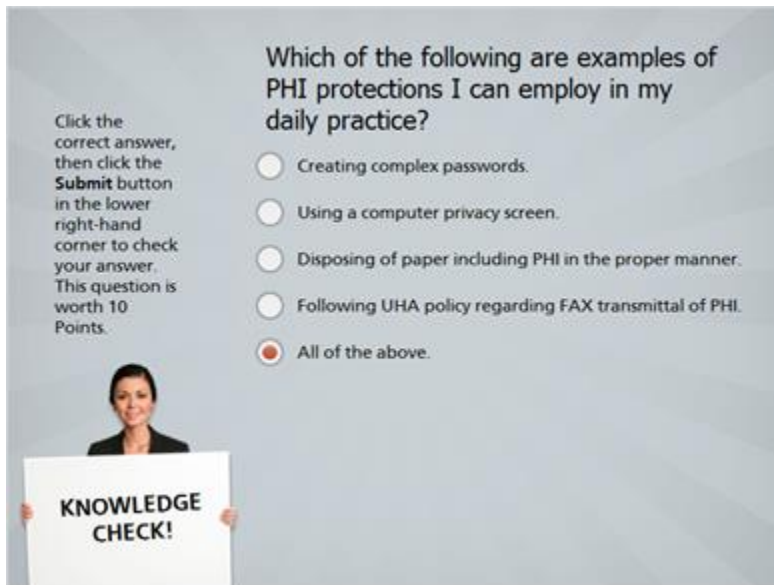
Questions? Contact UHA's IT Department.

1.54 Incident Reporting



1.55 Knowledge Check

(Multiple Choice, 10 points, unlimited attempts permitted)



Correct	Choice	Feedback
	Creating complex passwords.	That's not the correct answer. UHA is

	<p>responsible to provide support for protecting patient privacy and employees should become familiar with policy and regulations related to privacy so they can utilize the best practices in maintaining that privacy. Please try again.</p>
Using a computer privacy screen.	<p>That's not the correct answer. UHA is responsible to provide support for protecting patient privacy and employees should become familiar with policy and regulations related to privacy so they can utilize the best practices in maintaining that privacy. Please try again.</p>
Disposing of paper including PHI in the proper manner.	<p>That's not the correct answer. UHA is responsible to provide support for protecting patient privacy and employees should become familiar with policy and regulations related to privacy so they can utilize the best practices in maintaining that privacy. Please try again.</p>
Following UHA policy regarding FAX transmittal of PHI.	<p>That's not the correct answer. UHA is responsible to provide support for protecting patient privacy and employees should become familiar with policy and regulations related to privacy so they can utilize the best practices in</p>

		maintaining that privacy. Please try again.
X	All of the above.	Correct! UHA is responsible to provide support for protecting patient privacy and employees should become familiar with policy and regulations related to privacy so they can utilize the best practices in maintaining that privacy.

1.56 Non-Compliance



1.57 Consequences



What are the significant consequences for violating HIPAA and state privacy laws?

For UHA:

- Civil fines and penalties
- Impact on UHA and Stanford's reputation
- Increased regulatory scrutiny and monitoring

For individuals:

- **Civil monetary penalties (from \$100-50,000 per violation)**
- Criminal prosecution and jail time (up to 10 years)
- Disciplinary action up to and including termination of employment/contract
- If you are a licensed individual, you may face further disciplinary action by your licensing board

1.58 Reporting Requirements



What are the reporting requirements when a violation (i.e., a breach) occurs?

All impermissible uses, disclosures of PHI, or ePHI, are presumed to be breaches requiring timely reporting.

In addition, if a breach involves more than 500 individuals, UHA is required to notify the media.



1.59 Knowledge Check

(Matching Drag and Drop, 10 points, unlimited attempts permitted)

Let's see how much you've learned so far about what is (and isn't) compliant when working with PHI.

Printing your own (or your child's) medical record.	Okay only if you are accessing the data through your My Health account.
Viewing a patient's record out of curiosity.	Not okay, you should only access patient data needed for your job.
Sharing your password and logon.	Not okay, we never share our logons and passwords.
Talking about patients in public areas, during lunch or in an elevator.	Not okay, find a private place to talk and on a need-to-know basis only.

Using your mouse, drag the statements on the right to the matching phrase on the left. Once you have made all of your matches, click the **Submit** button to check your answers. This question is worth 10 points.

Correct	Choice
Printing your own (or your child's) medical record.	Okay only if you are accessing the data through your My Health account.
Viewing a patient's record out of curiosity.	Not okay, you should only access patient data needed for your job.
Sharing your password and logon.	Not okay, we never share our logons and passwords.
Talking about patients in public areas, during lunch or in an elevator.	Not okay, find a private place to talk and on a need-to-know basis only.

Feedback when correct:

That's right! You successfully matched the phrases.

Feedback when incorrect:

You did not make all the correct matches. Think about when it is, and isn't, okay to look Patient Health Information (PHI). Please try again.

1.60 Knowledge Check

(Multiple Choice, 10 points, unlimited attempts permitted)

LAST QUESTION!
Click the correct answer, then click the **Submit** button in the lower right-hand corner to check your answer. This question is worth 10 Points.

It is my responsibility to:

- ☐ Report non-compliance with UHA policy or Code of Conduct.
- ☐ Understand that email should be used for company business and may be monitored for use.
- ☐ Utilize proper measures to protect Patient Rights and Privacy.
- ☐ Ask questions if I do not understand whether authorization is needed to release information.
- ☒ All of the above.

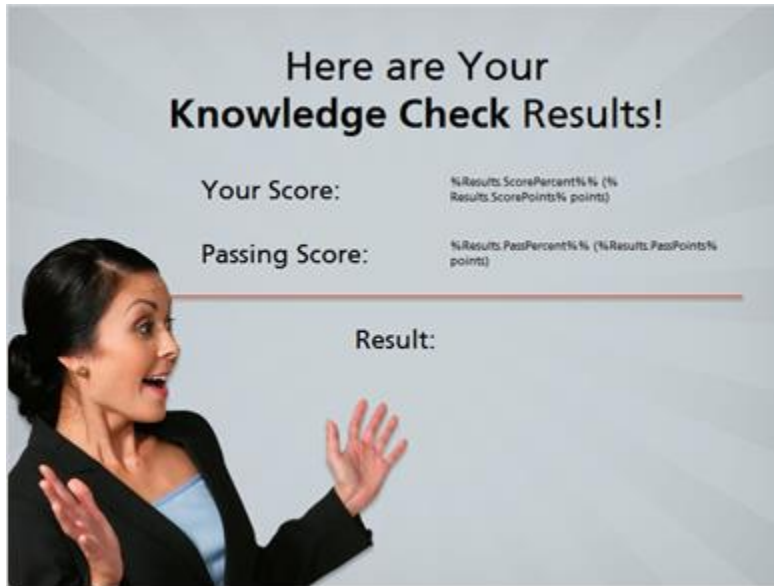
KNOWLEDGE CHECK!

Correct	Choice	Feedback
	Report non-compliance with UHA policy or Code of Conduct.	That's not correct. The Privacy and Security of PHI must be integrated into your daily duties. Following regulations and UHA policy will ensure the best patient care, enhancing our reputation as a premier health care service organization. Try again.
	Understand that email should be used for company business and may be monitored for use.	That's not correct. The Privacy and Security of PHI must be integrated into your daily duties. Following regulations and UHA policy will ensure the best patient care, enhancing our reputation as a premier health care service organization. Try again.

	Utilize proper measures to protect Patient Rights and Privacy.	That's not correct. The Privacy and Security of PHI must be integrated into your daily duties. Following regulations and UHA policy will ensure the best patient care, enhancing our reputation as a premier health care service organization. Try again.
	Ask questions if I do not understand whether authorization is needed to release information.	That's not correct. The Privacy and Security of PHI must be integrated into your daily duties. Following regulations and UHA policy will ensure the best patient care, enhancing our reputation as a premier health care service organization. Try again.
X	All of the above.	Correct! The Privacy and Security of PHI must be integrated into your daily duties. Following regulations and UHA policy will ensure the best patient care, enhancing our reputation as a premier health care service organization.

1.61 Results Slide

(Results Slide, 0 points, 1 attempt permitted)



Results for
1.10 Knowledge Check
1.21 Knowledge Check
1.26 Knowledge Check
1.33 Knowledge Check
1.40 Knowledge Check
1.47 Knowledge Check
1.51 Knowledge Check
1.55 Knowledge Check
1.59 Knowledge Check
1.60 Knowledge Check

Result slide properties

Passing Score

80%

1.62 Next Steps

Hey! You've completed the module! Thank you for taking the time to review this important information.

You may use the navigation buttons at the bottom to re-read any of the material, as needed. When you're ready, please close this window to return to HealthStream where you may now access the post-test.

If you have any questions about privacy or security, please contact the following individuals: UHA Compliance or , please contact the **UHA Director of Compliance**:



Carlos A. Cruz
UHA Director of Compliance
650.724.0326 (office)
CaCruz2@stanfordmed.org

Matt Berlin
Director, IT Planning and Operations
650.242.6856
mberlin@stanfordmed.org

joelarning.com design 