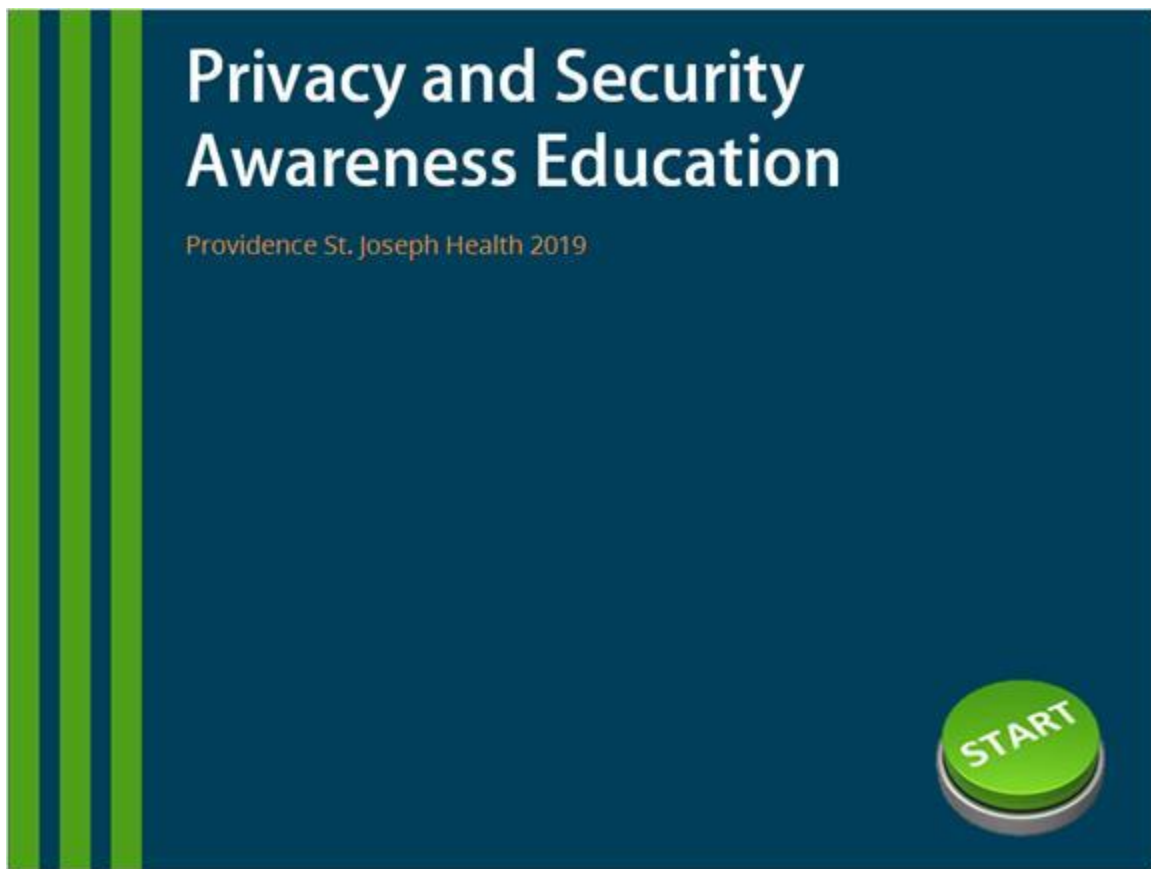


Privacy and Security Awareness Education 2019





Privacy. A Fundamental Patient Right

"The following scenario is true, but some of the details have been changed to protect the innocent, and the guilty. The setting is the cramped reception area of a small dental practice. The office manager, who also works the front desk, is on the phone there with a patient.

"Julie Jones? This is Dr. Burton's office. Your lab results are in and they indicate you've tested positive for an STD. You'll need to schedule an appointment as soon as possible with your primary care physician."

Her voice drifts over into the nearby waiting room. A few people look up from the magazines they've been flipping through. One of them, who happens to be a neighbor of Ms. Jones, arches an eyebrow and softly clucks her tongue. Information that should be confidential between this office and patient is now dangerously close to public knowledge. With this particular neighbor in the know, people in Julie's cul-de-sac will probably hear these results well before her current boyfriend.

Informing patients of test results is a normal and necessary part of the workday at every office that deals in healthcare. But in this case, **having that conversation where it can be overheard violates Ms. Jones' right to privacy.** A right protected by the law known as HIPAA."

[Continue reading the rest of the article here.](#)

Click Next to continue.



Course Topics

Privacy

- ☐ Overview of federal privacy laws
- ☐ Protected Health Information (PHI) and its definition
- ☐ How to appropriately access, use and share confidential information

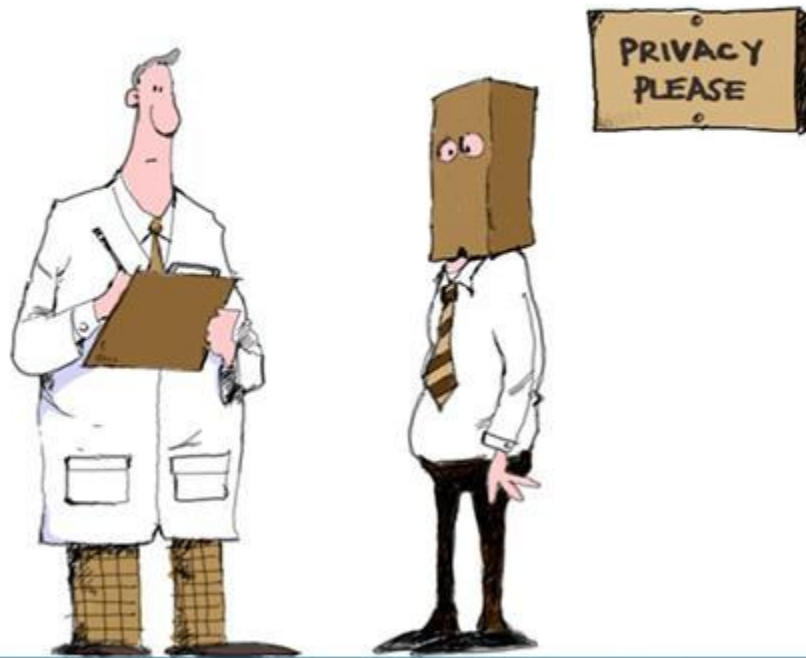
Security

- ☐ Reasonable and appropriate safeguards for protecting Providence St. Joseph Health (PSJH) systems and information
- ☐ Where and how to report security incidents

Click Next to continue.



Ensuring Our Patients' Privacy



Click Next to learn more about protecting our patients' privacy.



Laws that Govern Our Privacy

Protecting the privacy and security of our patient's health information is the right thing to do--and it is the law! Healthcare organizations must comply with federal and state privacy and security laws. Each workforce member plays a critical role in ensuring compliance and reducing the risk of incidents which may cause harm to patients, damage our organization's reputation, or result in monetary fines or legal action.

Click on the buttons below to learn about federal law.

HIPAA

HITECH

Click both buttons above then click Next to continue.

HIPAA (Slide Layer)



Laws that Govern Our Privacy

Protecting the privacy and security of our patient's health information is the right thing to do—and it is the law! Healthcare organizations must comply with federal and state privacy and security laws. Each workforce member plays a critical role in ensuring compliance and reducing the risk of incidents which may cause harm to patients, damage our organization's reputation, or result in monetary fines or legal action.

Click on the buttons below to learn about federal law.

HIPAA

HITECH

HIPAA is the federal Health Insurance Portability and Accountability Act of 1996. The goal is to improve portability of health insurance coverage, reduce healthcare fraud and abuse and to protect the privacy and security of healthcare information.

Click both buttons above then click Next to continue.

HITECH (Slide Layer)



Laws that Govern Our Privacy

Protecting the privacy and security of our patient's health information is the right thing to do—and it is the law! Healthcare organizations must comply with federal and state privacy and security laws. Each workforce member plays a critical role in ensuring compliance and reducing the risk of incidents which may cause harm to patients, damage our organization's reputation, or result in monetary fines or legal action.

Click on the buttons below to learn about federal law.

HIPAA

HITECH

The Health Information Technology for Economic and Clinical Health (HITECH) Act, was signed into law on February 17, 2009. HITECH was created to promote the adoption and meaningful use of health information technology as well as strengthening privacy and security protections.

Click both buttons above then click Next to continue.



Protected Health Information

Protected Health Information (PHI) is information, whether oral or recorded in any form or medium that is created or received by a health-care provider, health plan or health-care clearing house and relates to the past, present or future physical or mental health or condition of an individual or past, present or future payment for treatment and care to an individual.

There are [18 unique identifiers](#) associated with PHI. *All 18 identifiers must be removed for the information to be considered de-identified.*

Hover your mouse over "18 unique identifiers" then click Next to continue.

18 (Slide Layer)



Protected Health Information

Protected Health Information (PHI) is information, whether oral or recorded in any form or medium that is created or received by a health-care provider, health plan or health-care clearing house and relates to the past, present or future physical or mental health or condition of an individual or past, present or future payment for treatment and care to an individual.

There are 18 unique identifiers associated with PHI. *All 18 identifiers must be removed for the information to be considered de-identified.*

- | | |
|--|---|
| 1. Names | 12. Vehicle identifiers and serial numbers, including license plate numbers |
| 2. All geographical identifiers smaller than a state | 13. Device identifiers and serial numbers |
| 3. Dates (other than the year) directly related to an individual | 14. Web Uniform Resource Locators (URLS) |
| 4. Phone numbers | 15. Internet Protocol (IP) address numbers |
| 5. Fax numbers | 16. Biometric identifiers, including finger, retinal and voice prints |
| 6. Email addresses | 17. Full face photographic images and any comparable images |
| 7. Social Security Numbers (SSN) | 18. Any other unique identifying number, characteristic, or code except unique code assigned by the investigator to code the data |
| 8. Medical record numbers (MRN) | |
| 9. Health insurance beneficiary numbers | |
| 10. Account numbers | |
| 11. Certificate/license numbers | |

Hover your mouse over "18 unique identifiers" then click Next to continue.



Law Enforcement



When Law Enforcement requests patient information.

- ☐ Workforce members should understand the [patients' rights](#) regarding the disclosure of their personal or medical information at the request of law enforcement or other government agents.
- ☐ Workforce members must be polite when approached by law enforcement or government agents who may arrive on-site.
- ☐ Workforce members should not destroy, conceal, or alter documents in anticipation of or following a request by law enforcement or government agent.
- ☐ Workforce members should not provide any false or misleading statements to law enforcement or government agents.

Click "patients' rights" above to review then click Next to continue.



Law Enforcement



When Law Enforcement requests patient information.





- ☐ Disclosure of a patient's personal or medical information to law enforcement or government agents ***should not occur unless*** the facility has one of the following:
 - A written authorization by the patient;
 - A valid court order; or
 - A valid search warrant.
- ☐ The disclosure of patient information without the appropriate authorization or court documents could *violate federal or state privacy rules.*
- ☐ It is important that workforce members immediately notify their supervisor if approached by law enforcement so that the agent's request can be handled appropriately through facility procedure.

Click the X in the upper right hand corner to close this slide or Next to continue.

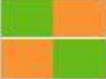


Consequences of Violating Patient Privacy




- ☐ The organization is required and committed to investigate potential violations of laws, policies, standards or procedures. Any corrective action will be based on the facts and circumstances of the violation.
- ☐ Violations may result in disciplinary action up to and including termination of employment and could result in fines, civil and/or criminal penalties.
- ☐ All workforce members should know how to appropriately disclose and/or access the [minimum necessary](#) information with those who are on a need to know basis. Our policies prohibit workforce members from accessing any records unless it is required to do their job.
- ☐ This will help all of us in doing our best to protect patient privacy and to avoid these consequences.

Click "minimum necessary" above to review then click Next to continue.



Consequences of Violating Patient Privacy



Minimum necessary is a standard that is used in the Privacy Rule to determine appropriate access and use of PHI for non-treatment purposes (such as payment and health-care operation functions). It requires that a covered entity take reasonable steps to limit the use, disclosure of, and requests for, PHI to the minimum amount of PHI necessary to perform its intended purpose. For example, if you do not need access to a patient's SSN to do your job, then you should not have access to the SSN in Epic (or anywhere else).

In short, if you do not need a particular patient identifier to do your job, you should not use or have access to that identifier. <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/minimum-necessary-requirement/index.html>

Click the X in the upper right hand corner to close this side or Next to continue.



Electronic Health Record (EHR)

There are many advantages of an EHR for our patients and the organization. However, the same advantages can also lead to the inappropriate access, use and sharing of PHI.

Before EHRs, it was time-consuming to access patient health information and even more time consuming to disclose it. Now with only a couple clicks of the mouse, workforce members can access and share patient records within seconds.

Because of this, it is important for us to understand what we can and cannot do in our EHRs to stay compliant and provide our patients the privacy they deserve.

Along with yearly education, our organization takes privacy a step further by **proactively** monitoring patient records in the EHR.

Click Next to continue.

Test Your Knowledge

I could be terminated for inappropriately accessing, using or disclosing patient health information.

☒ True

☐ False

You must answer correctly before you are able to move on.



Information Security Awareness

Triple venti half-
sweet non-fat
caramel machiato
for 083d9a270-
e6e16b2f.bb08d-
35067a2e5f.

I always **ENCRYPT**
my name in
public places
just to be safe.



Click Next to learn more about protecting our patients' privacy.



General Statements



- ☐ PSJH monitors the use of all PSJH information systems and all access to PSJH electronic data.
- ☐ Workforce members should have no expectation of privacy with regards to content or use of PSJH systems. This includes internet usage, communications and or transactions made that are of a personal nature while on our networks.
- ☐ All workforce members are obligated to cooperate with PSJH investigations or remediation efforts related to information security incidents.

Click Next to continue.



Password Protection

Passwords are the most common method used to secure access to information. It is important that you, as a PSJH workforce member, have a strong password and maintain the confidentiality of your password.

- ☐ PSJH Policy requires all passwords to be at least 8 characters and include three of the four listed: 1 upper case, 1 lower case character; at last 1 number, at least 1 symbol (!, @, #) and NOT contain any part of the user name (or user ID).
- ☐ Do not share your password. No workforce member, including support staff or management is allowed to request your login credentials.
- ☐ Your PSJH credentials should never be used on third party systems.
- ☐ Do not re-use your passwords.
- ☐ Use the approved Password Manager - Password Safe to store all your passwords for work.
- ☐ Using functionality available within a browser to store logins to any system, site, or application is never a good practice. Anyone else that logs into that computer will have access to sites using your credentials.

Click Next to continue.

Test Your Knowledge

Passwords should be “strong” and contain characters, numbers and symbols.

☒ True

☐ False

You must answer correctly before you are able to move on.



Mobile Devices

The use of wireless mobile devices for business related activities must conform to company policies and standards, including security, compliance, HIPAA, and PCI/DSS.

- ☐ All mobile devices on the PSJH network must comply with PSJH security standards including anti-virus, password protection, and encryption.
- ☐ Storage of, or accessing PSJH information or information systems on mobile devices requires the device to be approved for use and that the device comply with all PSJH security standards including anti-virus, password protection, and encryption
- ☐ Contact the Service Desk immediately if a device is lost or stolen



Click Next to continue.



Social Threats: Email Phishing and Phone Scams

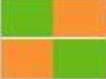
YOU are the first line of defense! Think before you click and ***always*** report suspicious emails.

- ☐ All mobile devices on the PSJH network must comply with PSJH security standards including anti-virus, password protection, and encryption.
- ☐ Storage of, or accessing PSJH information or information systems on mobile devices requires the device to be approved for use and that the device comply with all PSJH security standards including anti-virus, password protection, and encryption
- ☐ Contact the Service Desk immediately if a device is lost or stolen

Phishing Email
Example


Click the box above to move forward.

Example (Slide Layer)



Social Threats: Email Phishing and Phone Scams

Can you call out what details in the email make it phishing?



Mon 9/24/2018 8:06 AM

Delivery Notification <do-not-reply@freightinternationalservices.com>

Package Undeliverable

To: [redacted]

Delivery Notification

Order: SGH-9226-99950127

Dear Customer,

Your parcel has arrived at the post office. Our courier attempted but was unable to deliver the parcel to you.

To receive your parcel, please go to the nearest office and show this receipt.

[GET AND PRINT RECEIPT](#)

Thank you

Click the email above to show the details of what makes it a phishing attempt.

Details (Slide Layer)



Social Threats: Email Phishing and Phone Scams

Did you identify some or all of the details that make this a phishing email?

Mon 9/24/2018 8:06 AM

Package Undeliverable

To: [Redacted]

Delivery Notification

Order: SGH-9226-99950127

Dear Customer,

Your parcel has arrived at the post office. Our courier will deliver the parcel to you.

To receive your parcel, please go to the nearest office of our company.

Thank you

Do you recognize the sender?
Were you expecting a package?
Were you expecting the email?

Generic message without useful information.

Ambiguous greeting should alert you!

Company name and contact info should be present.

GET AND PRINT RECEIPT

While the links match, freight invoices are typically attached and not downloaded.

Click to follow link

Click Next to continue.

Next



Social Threats: How to Identify and Report

Whether you're expecting a delivery or not, there would be a lot more official information along with company information and logos. And, of course, rarely should you have to click a link or download something just to identify what deliver might have been missed.

Phishing Emails

Phishing Phone
Calls

Click both buttons above then click Next to continue.

Emails (Slide Layer)



Social Threats: How to Identify and Report

Whether you're expecting a delivery or not, there would be a lot more official information along with company information and logos. And, of course, rarely should you have to click a link or download something just to identify what deliver might have been missed.

Phishing Emails

Phishing Phone Calls

How to identify phishing emails:

- ☐ Poor grammar / spelling
- ☐ Unknown sender (address or domain) - hover over From / and links -
- ☐ Phishers can spoof email addresses and signatures belonging to our coworkers, patients and business partners.
- ☐ Appeals to emotions / urgency
- ☐ Requests info from you

Reporter button:

- ☐ If you get a suspicious email click on this button in the ribbon and it will be reported to the PSJH Cyber Defense Team.



Click both buttons above then click Next to continue.

Phone calls (Slide Layer)



Social Threats: How to Identify and Report

Whether you're expecting a delivery or not, there would be a lot more official information along with company information and logos. And, of course, rarely should you have to click a link or download something just to identify what deliver might have been missed.

Phishing Emails

Phishing Phone Calls

How to identify phishing phone calls:

- ☐ Just like with phishing emails, fraudsters often use the phone in an attempt to gather information.
- ☐ Never trust called ID - just like with email the bad guys can spoof phone numbers
- ☐ Usually they want money, information or access to your computer - or all three
- ☐ If you believe a phone call is an attempt to get information from you, hang up!
- ☐ If you supplied the caller with any information contact the Service Desk immediately!

Click both buttons above then click Next to continue.

Test Your Knowledge

Appealing to your emotions, contains poor grammar, is from a strange sender address or domain are all warning signs of a phish.

☒ True

☐ False

You must answer correctly before you are able to move on.



Electronic Communications

Email and Texting



- ☐ Use of personal email to transmit or store PSJH information is against policy
- ☐ To prevent viruses, malware and other disruptions to PSJH information systems, users must avoid opening suspicious emails and accessing suspicious or inappropriate websites.
- ☐ **#secure#** - if you need to send something to an authorized third party and it contains confidential information, including PHI, you must use #secure# in the subject line
- ☐ DLP blocking / reviewing of all emails sent - PSJH employs the use of a tool that reviews all emails being sent outside of PSJH. Emails are scanned and then blocked when they contain confidential information.
- ☐ Texting is not secure! Texting of patient orders is prohibited regardless of platform utilized! Texting guidelines: [text messaging](#) and [text paging](#)

Click Next to continue.

Test Your Knowledge

Sending patient information via text message or text page is secure.

- ☐ True
- ☒ False

You must answer correctly before you are able to move on.

Test Your Knowledge

When working on your personal mobile device, it is ok to send PSJH related information from your personal email account.

- ☐ True
- ☒ False

You must answer correctly before you are able to move on.



Cloud Storage

Public cloud service providers are NOT **Covered Entities** and are not authorized to have access to our data. The use of online storage services such as Google and Dropbox is against policy. The current and only approved IT solution for online storage is Microsoft OneDrive.

There are many risks associated with using online storage sites. Including the accidental disclosure of patient information.

- ❑ Often User Agreements with such online storage sites are written to allow the provider to access and or share data stored there with others as they deem appropriate and necessary.
 - Could insert specific language from Google User Agreement here as example - terms of service, data stored can be used for the purpose of operating, promoting and improving (its) services, and to develop new ones.
- ❑ Oregon Health & Science University (OHSU) agreed to a multi-million settlement with OCR for using Google (online storage site). The Department of Health and Human Services found that there was no contractual agreement, or Business Associate Agreement (BAA) in place between Google and OHSU to use or store data with the service provider.

Click Next to continue.



Cloud Storage

Public cloud service providers are NOT **Covered Entities** and are not authorized to have access to our data.

Dropbox is against policy.
Storage is Microsoft OneDrive.

There are many risks of
accidental disclosure.

Covered Entity:

A health plan, health care clearing house, or health care provider who transmits any health information in electronic form in connection with a transaction covered by HIPAA.

- ❑ Often User Agreements with such online storage sites are written to allow the provider to access and/or share data stored there with others as they deem appropriate and necessary.
 - Could insert specific language from Google User Agreement here as example - terms of service, data stored can be used for the purpose of operating, promoting and improving (its) services, and to develop new ones.
- ❑ Oregon Health & Science University (OHSU) agreed to a multi-million settlement with OCR for using Google (online storage site). The Department of Health and Human Services found that there was no contractual agreement, or Business Associate Agreement (BAA) in place between Google and OHSU to use or store data with the service provider.

Click Next to continue.

Test Your Knowledge

Posting files to unapproved cloud storage solutions is OK, as long as there is no PHI contained in them.

- ☐ True
- ☒ False

You must answer correctly before you are able to move on.



Payment Card Information (PCI)

What is PCI DSS?

The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that accept payment cards. It was created by the major credit card brands including:


- Visa
- MasterCard
- American Express
- Discover
- JCB



Payment Card Information must be protected to be compliant with the Payment Card Industry Data Security Standard (PCI DSS). Per the PSJH policy, it is prohibited to write down or in any way store anything but the *last four digits* of the PAN.

Hover over the photo to enlarge then click Next to continue.

Role (Slide Layer)




Payment Card Information (PCI)

Your Role and Obligation

It is prohibited to write down or in any way store any but the last four digits of the PAN. It is NEVER ok to write down or record the CCV (Card Verification Code). When handling a patient or customer's payment card information, it is **your responsibility** to exercise a reasonable amount of care in protecting that information from disclosure.

The following DOs and DON'Ts pertain to recording the cardholder data and the physical handling of printed material and the card themselves:

DO's	DON'Ts
<ul style="list-style-type: none"><input type="checkbox"/> Do redact all but the last four digits of the PAN<input type="checkbox"/> Do securely destroy payment card information once it is processed	<ul style="list-style-type: none"><input type="checkbox"/> Do not write down the card verification code or value<input type="checkbox"/> Do not write down the PAN<input type="checkbox"/> Do not leave the actual card unattended<input type="checkbox"/> Do not leave material containing full PANs unattended<input type="checkbox"/> Do not use email or other electronic means to send or forward sensitive cardholder information



Hover over the photo to enlarge then click Next to continue.



Payment Card Information (PCI)

If you have access to payment card information, never include payment card information in an email, text or instant message. If a patient sends their payment card information via those means, do not reply or forward that information.

Dispose of payment card documents using a micro shredder, cross cut shredder, or designated confidential-document-disposal bin.



Click Next to continue.



Payment Card Information (PCI)

Secure Payment Devices

- ☐ Personally owned devices may not be used as mobile Point of Sale (mPOS) devices, or use Mobile Card Readers to conduct PJSJH business purchases.
- ☐ It is important to be aware of attempted tampering or replacing point-of sale devices in PJSJH environment.
- ☐ Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices.
- ☐ Do not install, replace or return devices without verification or authorization.
- ☐ Be aware of suspicious behavior around devices.
 - For example, attempts by unknown persons to unplug or open devices.

Payment Card Information Key Points:

- ☐ Please refer to policy [PROV-FIN-526](#)
- ☐ Do not write down or record sensitive payment card information.
- ☐ Do not send sensitive payment card information, especially via email, text or other electronic means.

Click Next to continue.

Test Your Knowledge

When is it OK to email credit card numbers?

- ☒ Never
- ☐ Sometimes
- ☐ Always
- ☐ Emergencies

You must answer correctly before you are able to move on.



Physical Security: General Information

Physical Security is *everyone's* responsibility. The following are actions that you can take to help ensure PSJH ministries/facilities are secure:

- ☐ Always wear your badge on PSJH property.
 - It is OK to inquire when someone is not complying with this requirement in a friendly and professional manner.
- ☐ Prevent unauthorized individuals from entering or "piggybacking" confidential areas within the ministry/facility.
 - It is OK to inquire in a friendly and professional manner if someone does not look familiar and to validate their authorization to enter the ministry/facility.
- ☐ Do not loan out your keys or access cards, and if they are lost or stolen report it immediately to your local security personnel.
- ☐ Confidential information in hardcopy form must be kept in a locked cabinet/office when left unattended and should be shredded before disposal or placed in designated shredding bins provided by the local ministry.
- ☐ If you observe something that does not quite look, feel or seem right, it probably isn't. When in doubt, **REPORT IT** to your local physical security department.

Click Next to continue.



Physical Security: General Information

Immediately report privacy and security incidents or suspicious activity.

Security incidents to report are, but not limited to:

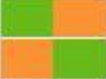
- ☐ Any suspicious persons or behavior
- ☐ Inappropriate access and disclosure of PHI
- ☐ Unauthorized access or use of computer systems
- ☐ Suspicious computer or login account activity
- ☐ Unauthorized access to secure locations
- ☐ Loss or theft of PSJH devices or removable media

Privacy incidents to report are, but not limited to:

- ☐ Inappropriate access to or disclosure of a patient record, including your co-workers'
- ☐ PHI posted on a social media site
- ☐ Confidential fax sent to wrong recipient
- ☐ Hospital discharge or clinic visit summary paperwork given to the wrong patient
- ☐ PHI discussed in a public place
- ☐ Unsecured PHI left in a vehicle

Report To...

Click the button above then click Next to continue.



Physical Security: General Information

Immediately report privacy and security incidents or suspicious activity.

Report incidents and concerns to:

- ☐ Your immediate supervisor
- ☐ Service Desk
- ☐ Privacy officers
- ☐ PSJH Integrity Hotline
- ☐ Information Security
- ☐ Payment Card Information incidents should be reported to the Integrity Hotline or Information Security

Click the button above then click Next to continue.



Your 2019 Commitment

As workforce members of our communities, the people we serve place an enormous amount of trust in us. Privacy and security are an important part of how we serve and represent our core values in action.

Each workforce member is responsible for maintaining the confidentiality, integrity and availability of PSJH's information. Our privacy and security policies ensure we are following the ethical commitments, laws, rules and regulations that govern our business conduct, and it helps to discourage, prevent and identify violations.

I, **Enter Your Full Name Here.**, reaffirm my commitment to the organization's *Acceptable Use policy and *Confidentiality Agreement.

**To review these documents, please contact your local privacy or security office.*

Submit

Click Submit to continue.

Your 2018 Commitment

Thank you **%textentry%** ! Your continued efforts in supporting our organization to fulfill our commitments to the patients and communities we serve is greatly appreciated.

Thank You

Click Next to continue.

THE END

Privacy and Security Awareness Education

Providence St. Joseph Health 2019

