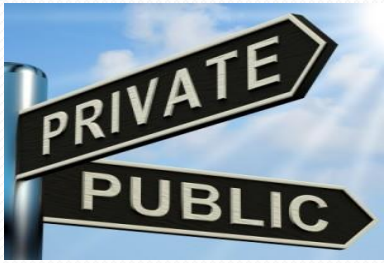
HIPAA PRIVACY & SECURITY TRAINING

HIPAA Basics

PRIVACY TRAINING

Objectives



- Gain an understanding of the basics of the HIPAA privacy rule
- Gain an understanding about what constitutes Protected Health Information (PHI)
- Gain an understanding of the Minimum Necessary rule
- Gain an understanding of patients' rights under HIPAA

HIPAA:
Health Insurance Portability & Accountability Act

- HIPAA protects patients' right to ***privacy***
- Protects patient information from unauthorized
  - ***Use***
  - ***Access***
  - ***Disclosure***
- Enforced by the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services
- States' privacy standards may be more strict than HIPAA

Who must comply with HIPAA?

- **Covered Entity**: Healthcare Providers, such as RCCH, who transmit health information in a HIPAA electronic form, such as in submitting claims for payment for services
- **Business Associate:** A person or entity, other than a member of a covered entity's workforce, who creates, receives, maintains or transmits protected PHI on behalf of RCCH
- **BA Subcontractor:** A person or entity under contract with a Business Associate who creates, receives, maintains or transmits protected PHI
- An entity may be a Covered Entity and may also provide services which place it in a category of a Business Associate

Your Responsibilities

As a member of RCCH's workforce, you are responsible for following privacy policies and procedures.

Privacy policies and procedures require you to:

- ***Collect, use, and disclose*** PHI for reasons that are for a legitimate job function, support the mission of RCHP, and are allowed by law.
- Disclose only the ***minimum necessary*** amount of information and only as permitted.
- ***Access*** information only for authorized purposes.
- ***Report*** suspected privacy violations or incidents.
- ***Comply*** with all applicable privacy laws.

What is Protected Health Information (PHI)?

Any information about a patient that comes from a patient, a health care provider or payor, relates to patient's past, present or future healthcare, and could be used **to identify a patient**. Examples of PHI* include:

Name	Medical History
Birth Date	Medications
E-mail address	Clinical Notes
Physical Address	Medical Record Number
Social Security Number	Admit/Discharge Date
Phone Number	Diagnosis

*other information may constitute PHI, such as x-rays or other digital images

Minimum Necessary Standard

HIPAA requires health care workers to use the ***minimum amount of PHI necessary*** to do their jobs efficiently and effectively.

Ask yourself:

- Do I need this information to do my job?
- Do I need to share this information with anyone else?
- What is the least amount of information I or my coworker need to do our jobs?

Access ONLY that information you need to *do your job*. *

Share information ONLY with *others who need it to do their jobs*.

* **RCCH's workforce is also prohibited from accessing their own medical records without requesting access as permitted under HIPAA.**

When is it Appropriate to Disclose PHI?

- HIPAA allows us to use or disclose PHI when we have a ***written authorization*** from the patient
- HIPAA allows use to use or disclose PHI without a written authorization from the patient in the following circumstances:
  - For the ***Treatment*** of the patient ; this includes for referral purposes
  - In order to receive ***Payment*** for our services
  - For the ***Operations*** of the hospital (e.g., quality assurance, financial operations, etc.)
  - Other specific exceptions (required by law, DHHS, etc.)
- HIPAA allows us to use or disclose PHI without a written authorization in certain limited instances when the patient has had an opportunity to object or opt-out, such as for fund-raising, facility directories or disclosures to or in the presence of patient family or friends
- HIPAA allows disclosure to a business associate after execution of a business associate agreement
- All authorizations and requests for PHI should be directed to the **HIM Department.**

Patient Authorization

Facilities ***must obtain authorization*** from patients before using or sharing their PHI for reasons other than ***treatment, payment, or health care operations.***

✦ An authorization from the patient must:

- Be **in writing and signed** (may be electronic)
- Be **in plain language**
- **Specify what** PHI will be used or disclosed
- **Specify who** will be disclosing and receiving the PHI
- Have an **expiration date**
- Inform the patient of his or her **right to revoke** the authorization

What YOU can do to Protect Patients' Privacy

Treat information as you would treat your own personal information.

- ✓ Do NOT discuss patients in public areas such as elevators, cafeteria lines, etc.
- ✓ Do NOT leave information about a patient in common areas.
- ✓ Do NOT look at patient information unless it is required to perform your job duties.
- ✓ Do NOT look up information about friends, family or others except as permitted
- ✓ Do NOT take records home without training and authorization.
- ✓ ALWAYS close curtains and speak softly when discussing treatments.
- ✓ ALWAYS log off and lock unattended computers.
- ✓ ALWAYS properly dispose of patient information.
- ✓ Keep laptops and other portable devices locked when not in use.
- ✓ Make sure doors and desks are locked as appropriate.
- ✓ Secure laptops and mobile devices at all times.
- ✓ Protect and don't share your User ID and Password.

"Most people don't do what they believe in; they just do what's most convenient, then they repent." – Bob Dylan

Additional Safeguards

- Properly dispose of paper documents containing PHI (promptly shred by placing in locked shredding bin or shredding onsite; incineration)
- Properly dispose of devices or equipment with PHI (demagnetize or destroy)
- Clean desk policy (when the desk is unattended, place all documents with PHI in a locked drawer)
- Log out of desktops or laptops when not in use
- Proper disposal of PHI not in either paper or electronic records (such as container labels , ID bracelets, bandaging with PHI)
- Prior to fax or email, verify address and recipient
- Promptly remove documents from Fax or printer
- Place Fax machines in private location
- Desktop screens should face away from public areas
- Do not to reveal PHI when leaving a voice-message
- Never deliver PHI by email or text which is not secured
- Do not download any PHI onto your desktop, laptop, smart phone or tablet except where authorized and encrypted
- Protect your password (do not share it or write it down)
- Verify the identity of any person requesting access to PHI (Practice employee, Business Associate, Patient, Patient Representative, Patient Authorized person, Payor, Other Healthcare Provider, Law Enforcement, Government agency)
- Monitor visitors in PHI sensitive areas
- Do not allow unauthorized persons access to areas or systems with PHI
- Use cyber-security awareness tips (do not open suspicious emails or download materials from suspicious emails, even if you know the email sender; do not download information from the internet without prior authorization)
- Social Media:
  - Never post patient information on any social media

Disclosures with an opportunity to agree or object:

- Facility directories: the patient must be given an opportunity to object to inclusion of information in the facility directory
- Disclosure to family, relatives, friends or others identified by the patient (may be informal consent)
- Fundraising purposes (patient must be given an opportunity to opt out of future fundraising communications)

Disclosures: Family or Friends

You may share patient information with family or friends:

- If the patient is conscious, with verbal permission and with an opportunity to object to discussions with the patient in presence of family or friends
- If incapacitated or unconscious, in your professional judgment if in the patient's best interest
- To identify, locate and notify family or caregivers
- Information relevant to patient care or payment
- Subject to the minimum necessary rule
- Use professional judgement and experience with common practice

Disclosures required by law or for the public benefit

- Required by law (statute, regulation or court order)
- Public health activity (preventing/controlling disease or injury, communicable disease, immunization registry, abuse/neglect, FDA regulation, employers); state law may require an opportunity to opt out
- Victims of abuse or neglect
- Health oversight activities (audits or investigations by agency or other government entity)
- Judicial/ administrative proceedings (if by order of court or tribunal; subpoena under certain circumstances)
- Law enforcement under certain circumstances
- Funeral directors, coroners, medical examiners
- Organ donation
- Research with IRB approval, preparatory to research or decedents
- Serious threat to health or safety
- Essential government functions (military, national security, inmates)
- Worker's compensation

Disclosures
Disaster Relief and Media

You may share patient information with a disaster relief organization:

- To notify family or other caregivers of patient's location, general condition, or death
- Patient permission is not necessary if it would impede relief organization response

You may not disclose patient information to the media except:

- When authorized in writing by the patient or
- If limited to directory information if

patient has not objected or restricted disclosure

Disclosures
Court Order/Subpoena
Use in Court

RCCH may respond to a Court ordered subpoena

- Disclosure limited to information requested

RCCH may respond to a subpoena without court order:

- Patient is a party
- Patient has received notice and had an opportunity to object
- Time for patient's objection has passed and any objections resolved
- Or a court has entered a Protective Order

RCCH may use patient information in court:

- RCCH is a party
- Subject to a protective order
- Subject to the minimum necessary rule and limited to relevance

Use of Personal Mobile Devices

- **Calls**
  - **DO NOT** make personal calls in treatment areas or other areas where discussions regarding patient information may be overheard
- **Texting**
  - **DO NOT** text patient information with your personal device
  - Standard texting accounts are **NOT SECURE;** use of an RCCH approved secure text service is required
  - **DO NOT** text patient orders or other information that is part of the patient record even with a secure encrypted text service
  - **DO NOT** communicate with a patient by text
- **Downloading**
  - **DO NOT** download patient records or other patient information to your personal device
- **Photos/Video**
  - **DO NOT** take photos or videos of patients or patient information with your personal device
  - **DO NOT** take "selfies" or group photos in a treatment area or other area where patient information may be visible in the photo

Emailing and Privacy

- **Emailing guidelines**
  - **DO NOT** send confidential information unless **absolutely necessary.**
  - **DO NOT** send **attachments containing PHI** without encryption.
  - **DO NOT** email PHI on a **personal or non-RCCH email** account.
  - **DO NOT** open or respond to suspicious emails, such as a "phishing" email. Phishing is an email which appears to be from a colleague or otherwise appears to be legitimate, but includes a request for protected information or directs you to a link that if "clicked" will download a virus, such as a Trojan virus or ransomware.
  - **DO** use ONLY encrypted E-mail to deliver patient information
  - **DO de-identify** the information if possible

Social Media

- **DO NOT** post or share patient information on any social media site, such as Facebook, Twitter, or Snapchat
- **DO NOT** “like,” “love” or otherwise respond to any patient comment, post or twitter relating to treatment provided by you or at RCCH
- **DO NOT** **“**friend” or otherwise respond to a patient invitation to your social media account (except to the extent the invitation is completely unrelated to any treatment or care at RCCH)
- **DO NOT** respond to any patient review or online public comments regarding treatment by you or at RCCH
- **DO disable** automatic sharing with social media sites to avoid any inadvertent posts that may disclose patient information

Marketing

- Marketing is:
  - a communication about a product or services that encourages recipient to purchase or use the product or service or
  - an arrangement between RCCH and another entity where RCCH discloses PHI in exchange for direct or indirect remuneration ($ or anything of value) to communicate about the other company's products or services and encouraging the use or purchase of the products or services
  - Exceptions:
  - Communications about network providers
  - Communications for treatment of patient
  - Communications for case management or care coordination, to direct or recommend alternative treatments, therapies, providers or care settings
- Authorization must disclose to the patient if remuneration is involved
- No authorization required if: face-to-face communication between provider and patient or for gift of nominal value to patient

Patient Rights under HIPAA

- Right to access records
- Right to request amendment of records
- Right to request communications by alternative means
- Right to request an accounting of disclosures
- Right to restrict uses and disclosures of information
- Right to receive Notice of Privacy Practices
- Right to object to or opt out of certain disclosures
- Right to submit a complaint regarding RCCH's privacy practices

Patient's Right to Access

- If a patient requests access to or a copy of his/her medical records:
  - Refer the patient to the appropriate form for requesting access to records in writing
  - RCCH must provide access except for certain limited circumstances
  - Access or a copy of records must be provided within a specified time period
  - Only the actual cost of reproducing and delivering the record may be charged

What is a Breach?

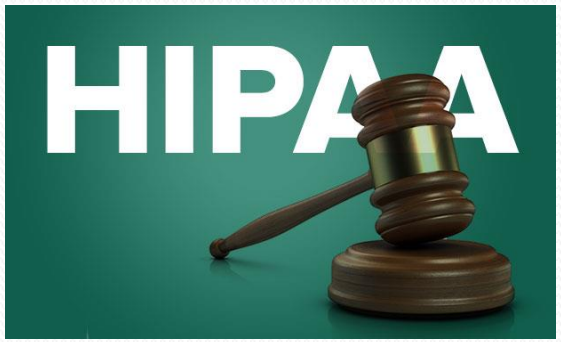
A Breach under HIPAA occurs when there is an:

- **Access, Use or Disclosure** of patient PHI for any reason not permitted by HIPAA. This includes any security incident that may compromise the confidentiality of the PHI.
- There are certain limited exceptions to a Breach. Whether an exception exists is a determination to be made by the RCCH Privacy Office.

Consequences for Breaches

RCCH takes seriously the responsibility to protect the privacy of its patients and their PHI in our care.

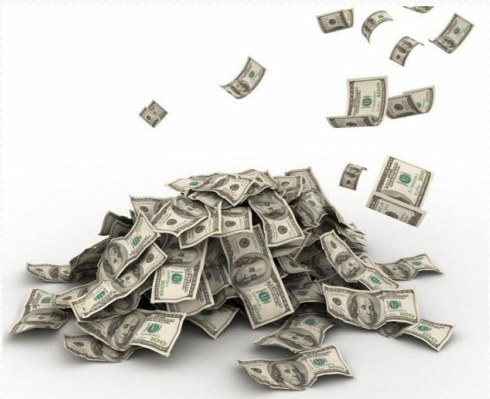
- Failure to adequately ensure the privacy of PHI can result in disciplinary action against you, up to and including:
  - Verbal or written warning
  - Re-training
  - Suspension
  - Termination/Dismissal
  - Lawsuits
  - Fines
  - Criminal charges and jail time of 1-10 years



Failure to report a violation is a violation!!

Business Impacts of a Breach

- Loss of Reputation
- Reporting Costs
- Lawsuits
- Fines & Penalties, civil and criminal
- Government Audits
- Attorney's Fees
- Upset Patients
- Analysis Costs
- Mitigation Costs



HIPAA Penalties

HIPAA Violation	Minimum Civil Penalty	Maximum Civil Penalty	Minimum Criminal Penalty	Maximum Criminal Penalty
Not due to willful neglect and corrected in 30 days after discovery	0	0	None	none
Individual did not know (and by exercising reasonable diligence would not have known) that he/she violated HIPAA	$100 per violation/ $25,000 per year	$50,000 per violation/ $1,500,000 per year		
Violation due to reasonable cause and not due to willful neglect	$1000 per violation/ $100,000 per year	$50,000 per violation/ $1,500,000 per year		
Violation due to willful neglect but corrected within thirty (30) days	$10,000 per violation/ $250,000 per year	$50,000 per violation/ $1,500,000 per year		
Violation due to willful neglect but not corrected	$50,000 per violation/ $1,500,000 per year	$50,000 per violation/ $1,500,000 per year		
Knowingly uses, obtains or discloses IHII without authorization			Up to $50,000 or 1 year imprisonment	$50,000 and 1 year imprisonment
Knowingly and under false pretenses uses, obtains or discloses IHII without authorization			Up to $100,000 or 5 years imprisonment	$100,000 and 5 years imprisonment
Knowingly with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm			Up to $250,000 or 10 years imprisonment	$250,000 and 10 years imprisonment

Reporting Breaches

If you are aware of or suspect a violation, you are required to ***immediately*** report it to any of the following:

- Your Facility Privacy Officer (FPO), Ethics & Compliance Officer (ECO), Regional Compliance Officer (RCO)
- Compliance Hotline (accepts anonymous reports)

www.RCCHHealth.com/Compliance

1-888-9CARE91

Supervisors are required to report any suspected violation reported by an employee.

- Do not investigate the incident on your own – **immediately report any suspected incident.**
- Any employee can report an incident.
- You are not required to speak to your supervisor before reporting an incident.
- RCCH does not retaliate against anyone reporting a suspected Breach

Examples of Potential Breaches

- Stolen laptop
- Lost smart phone
- Misplaced patient records

Loss of PHI or equipment containing PHI

Co-workers sharing passwords
Snooping in patient's record

Misuse of information and systems access

Misdirected faxes, mail and e-mails
Human error
Overheard conversations
Mix-up in discharge instructions
Phishing email attack

Accidental or unauthorized disclosures of PHI

HIPAA Security and RCCH Information Security Policies Training

RCCH Healthcare Partners

Objectives

- Gain an understanding of the basics of the HIPAA security rule
- Gain an understanding about what your role is in protecting the security of patient information
- Gain an understanding of strategies to prevent and identify cyber-security attacks
- Gain an understanding of the RCCH Information Security Policies

HIPAA Security Rule

HIPAA requires that RCCH, and you as its employee, maintain reasonable and appropriate **administrative, technical, and physical safeguards for protecting electronic PHI (ePHI)**.

- Ensure the confidentiality, integrity, and availability of e-PHI created, received, maintained or transmitted;
- Identify and protect against reasonably anticipated threats to the security or integrity of the information;
- Protect against reasonably anticipated impermissible uses or disclosures; and
- Ensure compliance by workforce.

Administrative Security Standards

- **Risk Analysis**: Periodic evaluations of threats to the PHI, security vulnerabilities and existing security safeguards, and recommendations for improving management of security risks.
- **Access**: Procedures for accessing ePHI by establishing a user's right of access to a workstation, the network, cloud-based databases and software applications.
- **Appropriate Access**: Procedures to determine that access to an employee is appropriate to support his or her role.
- **Access Termination**: Procedures to terminate access when employment ends or a business associate relationship ends.
- **Security Awareness Training**: Training of new employees and on-going training for existing employees concerning their role in safeguarding the confidentiality, integrity and availability of ePHI, including guarding against, detecting and reporting malicious software.

Administrative Safeguards (cont.)

- **Workforce Supervision**: Procedures for the authorization or supervision of workforce members who access or use ePHI or in locations where it may be accessed.
- **System Monitoring**: Procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.
- **Sanctions**: Appropriate sanctions against employees who fail to comply with the security procedures of the Company.
- **Incident Response**: Procedures for responding to, mitigating, and documenting suspected or known security incidents and any outcomes.
- **Contingency and Disaster Planning**: Procedures for ensuring continued availability of mission-critical information resources in the event of unforeseen circumstances (tornado, hurricane, flood, fires, terrorism, etc.)
- **Business Associate Obligations**: The Company ensures that its Business Associate Agreement contracts require that the Business Associate comply with the Security Rule, and as needed, provide Practice with access to its records to verify compliance.

Physical Security Standards

- **Physical Access Controls**: Procedures to limit physical access to ePHI and the facility(ies) in which it is housed and for authorizing appropriate access.
- **Physical Identification Validation**: Procedures to guard against theft or tampering and which address control and validation of a person's access to facilities and the network based on his or her role, including visitors, maintenance workers and vendors.
- **Physical Environment Controls**: Procedures to ensure appropriate physical security and protection of the environment in which ePHI is access, stored or transmitted. This includes locks, alarms, temperature controls, as needed, and fire response equipment.
- **Workstation Security**: Procedures to establish access to and appropriate use of Workstations and appropriate location.
- **Asset Security**: Procedures to track the receipt and movement within and without the facilities of hardware, including printers, copiers and scanners, laptops and portable devices like smart tablets and smart phones, and other electronic media that contain ePHI.
- **Asset disposition**: Procedures to address final disposition of media containing ePHI, including destruction, donation or lease termination, and removal of ePHI from such media prior to destruction, donation, return to leasing vendor, or repurposing for use within the facility.
- **Mobile Device Security**: Procedures to protect against loss or theft of ePHI contained or accessed on Mobile Devices.

Technical Security Standards

- **System Access and Configuration**: Procedures to limit access based on the workforce role or job, to assign unique user names and passwords for tracking and identifying user identity and authority, to terminate or modify user access based employment changes or in response to a security incident. Procedures to address remote network access over a secure VPN or other access method. Procedures to address system configuration and changes.
- **User Authentication**: Procedures to verify the identity of a person seeking access to the system and changes in authentication.
- **Password Management**: Procedures for assigning unique user names and passwords, periodic password changes, and appropriate password protection.
- **ePHI Integrity**: Procedures that protect ePHI from improper alteration or destruction, which include a mechanism to authenticate ePHI and corroborate that it has not been altered or destroyed in an unauthorized manner. These include Firewalls, vulnerability and patch management, malicious software prevention and detection devices, anti-virus applications and updates and employee training regarding methods to detect and avoid introduction of malicious software into the system.

Technical Standards (cont.)

- **Incident Reporting and Tracking**: Procedures for monitoring and auditing information system activity and detecting unauthorized or inappropriate access to the system and to ePHI, including regular audit log creation and review.
- **ePHI Storage**: Procedures for preventing the unauthorized disclosure, modification or destruction of data while in storage; encryption of stored ePHI when reasonable and appropriate.
- **ePHI Transmission**: Procedures to ensure that ePHI transmitted over electronic communications networks (including wireless networks) is not improperly accessed by unauthorized persons, altered or destroyed improperly; encryption of ePHI in transit.
- **Mobile Devices**: Procedures for ensuring that Mobile Devices which are used to access or transmit ePHI are tracked, maintained securely, secured with appropriate authentication, encrypted and configured with remote locating and data wiping features.

Your role in maintaining PHI Security

- **Security awareness training**
- **Desktop and network access**: Your desktop should be set to automatically time-out after a period of inactivity. Do not circumvent this setting. Ensure that your desktop screen is not facing a public area.
- **Building Access**: Keep your building passcard or key secure. If it is lost or stolen, notify your supervisor or the Privacy Officer immediately. Do not prop open any exit doors. Visitors and maintenance workers should be required to sign in and should be monitored while in the building.
- **Remote Access**: You may be authorized to access the network remotely. You may only do so through the authorized secure access point, such as the VPN. Do not allow any unauthorized person to access the network through this access point.
- Do not allow any unauthorized person access to the secure network.

Your role in maintaining PHI Security (cont.)

- **DO NOT** dispose of or re-purpose any hard-drive, flash drive, DVD or other portable storage device which contains PHI – this includes flash drives, printers, fax machines and scanners.
- **DO NOT** download PHI onto any unencrypted desktop, laptop, smart phone or tablet.
- Any electronic transmission of PHI should be encrypted, including email or text.
- Transfer or downloading of PHI onto a DVD or USB may only be done with approval and using an appropriately encrypted device.

Password Security

- You are assigned a **UNIQUE USERNAME AND PASSWORD**.
- **DO NOT** share this with anyone.
- **DO NOT** write it down or store it on your desktop.
- **DO** choose a password that is not easily guessed, with at least one number and one character and with at least the minimum number of
- Passwords should not include personal information such as birthdates, your name or that of your family members or pets, social security numbers or any other information about you which is easily obtained online or otherwise easily discoverable.
- You may be required to use a multi-factor authentication such as a password and fingerprint or other biometric.
- You will be required to update and change your password periodically.
- If you need to reset your password, contact the Security Officer for the reset procedures.

Password strength example

- Avoid using birthdays, names, pets, phone numbers, addresses, sports teams, company information or derivation of a common work (“P@$$word”)
- Instead consider a phrase with at least 1 capital letter, 1 number and 1 special character:

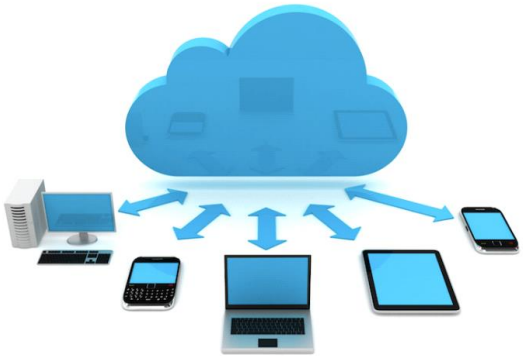
Examples:

Quote from a favorite book:

@ndMaxSaid!L3tthew1lDrumpu$$t@rt!!

Network and Device Security

- Your desktop, laptop or other device which is used to access the network must be configured under the supervision of the Security Officer.
- **DO NOT** leave any laptop or mobile device with PHI unattended in a public area, including a parked car.
- **DO NOT** bypass or circumvent configuration.
- **DO NOT** download unessential applications without authorization(e.g., games, photo sharing tools, peer-to-peer applications, social media)
- **DO NOT** remove or disable any antivirus installed on your device.
- **DO NOT** remove, bypass or circumvent any firewalls installed.
- **DO NOT** bypass RCCH backup procedures



Mobile Device Security

- **DO NOT** use an unapproved laptop, smartphone or tablet
- **DO NOT** leave your Mobile Device unprotected in a public location.
- **DO NOT** donate or dispose of your Mobile Device without prior approval from the Security Officer and performance by the Security Officer of data removal.
- **DO NOT** use a Mobile Device that does not support encryption if any ePHI is transmitted or stored on the device.
- **DO NOT** transmit unencrypted ePHI across a public network.
- **DO** ensure that your Mobile Device is password protected, the device locating feature is enabled, has a wiping feature in the event of a specific number of failed access attempts and remote wiping is enabled.
- **DO** disable any automatic sharing with social media sites such as Facebook.
- **DO** disable Bluetooth when in public settings. This provides a door for a hacker!

If your device is lost or stolen, contact your Security Officer immediately and activate the device locating feature, and if stolen or not located, activate remote data wiping

Removal of PHI Outside RCCH

- **DO NOT** remove PHI from RCCH premises on any portable device, such as a laptop, tablet, smart phone or flash drive without **PRIOR** approval

- **DO use safeguards**
  - Encryption of device and/or data required
  - Files password protected and 2 factor authentication if available
  - Physical security – do not leave in car, hotel room, or other public place
  - Tracking required and remote location, if available
  - Remote wiping, if available
  - Operating system and anti-virus updated

- Permitted only as necessary and approved based on:
  - RCCH assessment of risk to PHI when removed
  - RCCH policies and procedures regarding removal of PHI
  - RCCH safeguards to protect PHI

Remote Access to PHI

- **DO NOT** access to PHI remotely except with **PRIOR** approval
- **DO NOT** share access with another person, including family members
- **DO NOT** access remotely on a public device, such as a hotel business center
- **DO use safeguards:**
  - Passwords and 2 factor authentication
  - Secure remote connection, such as VPN
  - Account locked after a certain number of failed access attempts
  - Log off when unattended
  - Remote device anti-virus installed and updated
  - Remote device operating system software approved and updated

Internet and Email Security

- **DO NOT** send PHI over an open network.
- **DO NOT** send PHI through unencrypted email.
- **DO NOT** open suspicious email or open links in such email. Report any suspicious email to your Security Officer.
- **DO NOT** download programs or documents from public internet sites. Downloading documents or photos from the internet, especially from an unauthorized internet location, may result in downloading a virus.
- Ransomware and other viruses or malware which may permit hackers to either encrypt, steal or damage the data most frequently enter through phishing emails or other forms.

If you suspect you have been "hacked"
immediately contact
your supervisor and the Security Officer.

How to detect and what to do: phishing communications

- Messages may appear to come from a friend, co-worker, supervisor, company officer, your company, such as the IT, accounting or HR department, or a business that you use
- Not limited to email but may include interoffice "chat" services, text messages, or social media such as Facebook, Instagram or LinkedIn
- Be wary of unusual messages, use of poor grammar or spelling, urgent or unexpected requests from a co-worker or trusted source that you click on a link (such a Google docs or DropBox) or provide personal information or transfer funds
- **DO NOT** open or click on any link, respond by email, phone or text to provide any personal or confidential information, or transfer funds ***without separate verification***
- **IMMEDIATELY** report to your Privacy and Security Officers

Examples of phishing or other malicious communications

Malicious messages are not limited to email but may come in the form of text messages or other digital communications

Example: co-worker

Richard Sent Secure Email

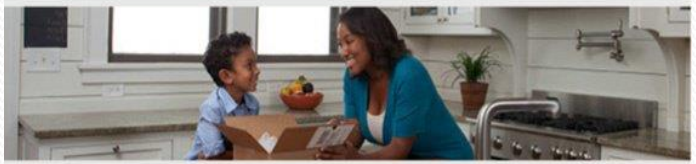
Read this Message from a Tablet or Mobile Device or Desktop or Laptop

Click Here from your device for instructions unique to your device.

Sincerely,
Richard Fletcher

The Google Apps Team

Example: Trusted vendor



Hi <customer>,

This is a follow-up regarding your package delivery:

- Tracking Number: 0p2uYq5RIho

The package contained in the above-mentioned shipment was not accepted at the destination address. Please contact your local UPS office and provide the printed delivery sticker, included in this email.

Please note that in case of a failure to contact your local UPS office within 21 days the parcel will be returned to sender.

Thanks so much for shipping with UPS.

Get the UPS My Choice app for Facebook

Download the UPS mobile app

Example: LinkedIn

Edward Johnson
Entrepreneur
3 hrs

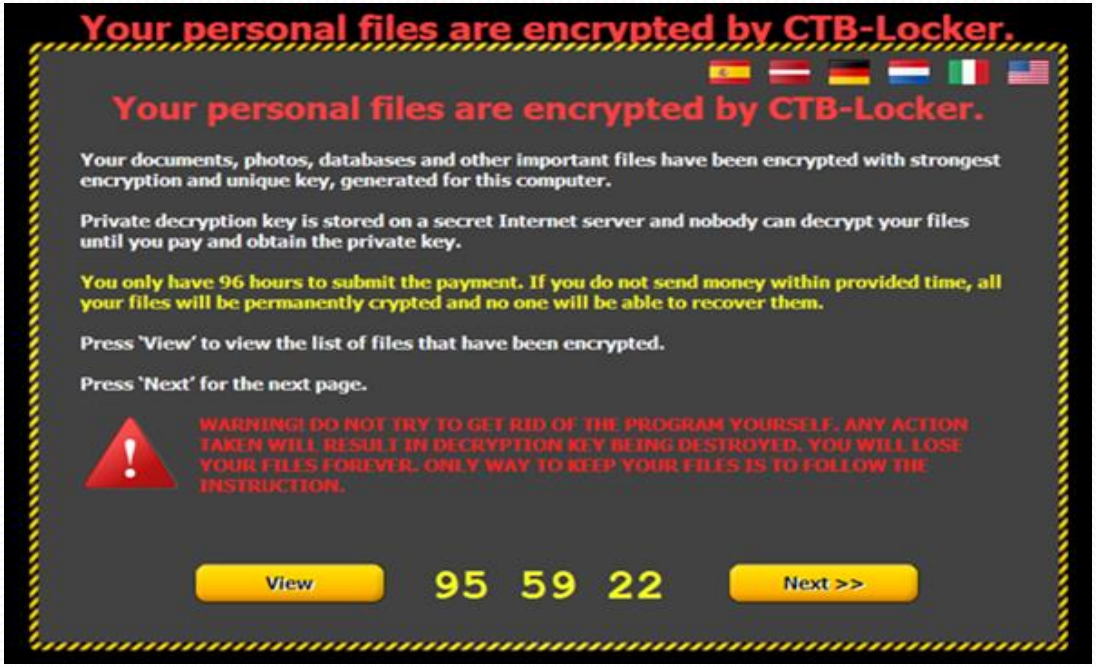
You join me, we both get paid! Creating a group for real estate investors, brokers, owners and agents! Drop your number here if you are interested!

12 Likes · 4 Comments

Like Comment Share

Ransomware and other malicious malware

- Ransomware and other malicious malware are software programs downloaded through phishing emails or other methods compromising access credentials
- It will access data, which many include PHI and encrypt to prevent access, may also copy, remove and /or alter



Information Security Policies

- There are twelve (12) Security policies that cover a wide array of topics.
- This presentation will help point out topics in the policies that are relevant to you.
- Note this presentation does not thoroughly cover all policies; it is meant to provide a high-level overview.
- Policies can be reviewed in detail on UltiPro here

IT.SEC.001 Information Security Organization

Key Points

Individuals authorized to access RCCH information and/or information processing resources shall:

- Remain aware of RCCH information security policies, standards, and operating procedures and of the risks and protective measures in their realm of control;
- Obtain appropriate authorization from the Business Owner(s) to access RCCH information and systems;
- Refrain from browsing files and information if they do not have permission for business purposes;
- **Understand granting access to RCCH information does not imply or confer authority to grant other users access to that information;**
- Comply with relevant laws and regulations with regard to information access and the operation of information security safeguards;
- Notify management of relevant issues, circumstances and/or weaknesses in information security safeguards.

IT.SEC.002 Human Resource Security

Key Points

- **Prior to Employment or Personnel Credentialing** - Background checks must be performed and the workforce member must sign a Security Agreement.
- **During Employment or Credentialed Service** – All workforce members must complete periodic training and ongoing security education.
- **Sanctions Policy** – All workforce members are subject to the sanctions policy.
- **Relationship Termination** – Managers must notify HR concerning any relationship termination.

- **Why is Human Resource Security important?**
  - Ongoing training and education is essential in IT Security due to the ever changing world of technology.
  - When relationships are terminated we need to ensure that access is removed.

IT.SEC.003 Asset Management

Key Points

- **Responsibility for Assets** - Business Owners are ultimately responsible for protection of organizational assets. All users are responsible for assisting Business Owners in these protection efforts.
- **Media Handling** – All users are responsible for the appropriate management, tracking, and secure disposal of removable media, such as flash drives, discs, etc.

- **Why is Asset Management important?**
  - RCCH is a custodian of confidential information (patient and employee information). We are responsible for protecting confidential information in our custody.
  - Proper media handling is a key component of information protection.

IT.SEC.004 Access Control

Key Points

- **Business requirements of access control -** Business owners are responsible for application level access controls.
- **User access** – Individuals should have the minimum access required to perform their job duties.

- **Why is Access Control important?**
  - Business owners should ensure that users only have access to what they need and nothing more.

IT.SEC.005 Encryption

Key Points

- We use encryption to secure emails and data to keep information protected.
- **Why is Encryption important?**
  - Encryption helps ensure that our computers and our company data is protected.
  - Any mobile media (Laptop, Flash Drive, etc.) must be encrypted. If you have questions on how to encrypt something or when you should encrypt something, please ask your local IT staff.

IT.SEC.006 Physical Security

Key Points

- **Physical Security** – Physical controls should be in place to prevent unauthorized individuals from accessing secure areas and information. Physical controls include things such as door locks, cameras, cable locks, etc.
- **Access Administration** – A process should be in place to grant authorized visitors temporary access to secure areas and information.
- **Removal of Assets** – Sensitive assets (PHI, PII, Credit Card Data) should not be removed unless all data has been appropriately wiped.

- **Why is Physical Security important?**
  - Physical security can be just as important as digital security. The easiest way for someone to get access to non-public data is to use your computer when you aren't looking.
  - If you aren't sure if you are meeting the previous controls related to your devices, ask your local IT what you should do instead.

IT.SEC.008 Communications Security

Key Points

- All sensitive information that is sent outside of the company network should be sent via secure means, such as encrypted e-mails, secure file transfer protocol (SFTP), etc.
- Only IT approved means should be used for transfer of sensitive data. If you aren't sure, ask before sending data!
- Personal accounts such as e-mail, instant messengers, and text messages should never be used to send or receive company data.
- Sensitive or non-public information should never be posted on social media. Keep your social media accounts focused on your personal life, not your work life!

- **Why is Communications Security important?**
  - Patients deserve and expect for their healthcare providers to properly store and use their information.
  - Patient and business data should be treated with the same amount of care that you would give to your own personal information.

IT.SEC.010 Supplier Relationships

Key Points

- Before entering into a relationship with third parties, an approved business purpose must be documented with an executed contract.
- All third parties must complete the appropriate approval process prior to being granted access.

- **Why is this important?**
  - It is imperative that we help ensure that sensitive information in our care is properly protected.
  - Having a properly executed contract helps our suppliers understand and comply with the established protections.

IT.SEC.011 Information Security Incident Management

Key Points

Any information security incidents or suspicious activity should be reported to your manager, local IT Director and/or the Helpdesk. For example:

- **Suspicious e-mails**
- **Unusual system activity, pop-ups, or messages**
- **Loss of company equipment (laptops, removeable media, etc.)**
- **Individuals lacking badges or escorts in sensitive areas.**

Why is this important?

- It is up to each RCCH employee to identify and report potential security incidents. The RCCH security team can respond to incidents more effectively if they are reported in a timely manner. Timely reporting of incidents can also help prevent the loss of sensitive data.

Conclusion

- RCCH needs **Your** Help in Protecting Our Patients' Privacy.
- We all want our privacy protected when we are the patient – ***it's the right thing to do.***
  - ➢ Don't be careless or negligent with PHI in **any** form.
- Treat a Patient's Information *as if it were your own.*
- _____
- *User attestation:*
- I attest that I have read and understand all of the education regarding HIPAA that is supplied in this document. I have no further questions regarding HIPAA or PHI and agree to comply with all state and federal laws related to HIPAA and PHI.
- Signature:_____ Date: _____
- Printed Name:_____
- Please return to the Facility Privacy Officer at Community Medical Center. Fax 406-327-4510