PROCARE
MANAGEMENT SERVICES ORGANIZATION

HIPAA & HITECH Training

Welcome
Compliance Training

- Section 1: HIPAA Privacy
- Section 2: HIPAA Security
- Section 3: HITECH
- Section 4: Reporting a Breach
- Section 5: Disciplinary Actions
- Section 6: PDT Obligations & Resources

PROCARE
MANAGEMENT SERVICES ORGANIZATION

HIPAA Privacy & Security

HIPAA PRIVACY

Protection for the privacy of Protected Health Information (PHI) effective April 14, 2003 (including standardization of electronic data interchange in health care transactions, effective October 2003)

HIPAA SECURITY

Protection for the security of electronic Protected Health Information (e-PHI) effective April 20, 2005

PROCARE
MANAGEMENT SERVICES ORGANIZATION

Privacy vs. Security

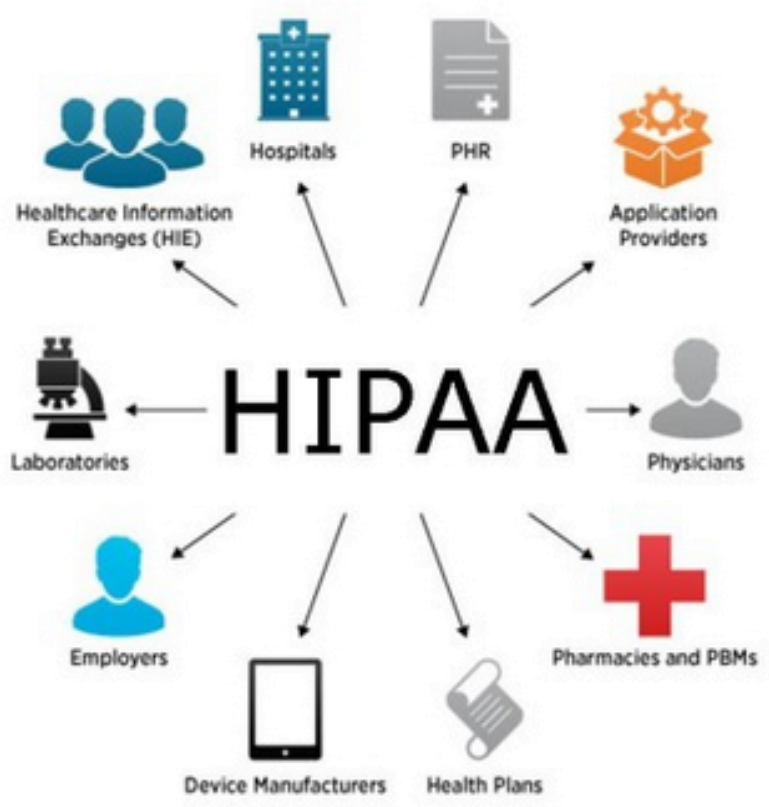
Privacy Rule

- Sets the standards for how covered entities and business associates (BAs) are to maintain the privacy of Protected Health Information (PHI)

Security Rule

- Defines the standards which require covered entities to implement basic safeguards to protect electronic Protected Health Information (e-PHI)

PROCARE
MANAGEMENT SERVICES ORGANIZATION



Section 1: HIPAA Privacy

PROCARE
MANAGEMENT SERVICES ORGANIZATION

HIPAA Privacy

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 requires that PDT, including all delegated entities, complete HIPAA training upon hire or contract and annually thereafter.

- What is HIPAA?
- Who has to follow the HIPAA law?
- What is considered PHI?
- How does HIPAA affect PDT?
- What does this mean to me?
- What are other uses and disclosures?
- How do we protect PHI?

PROCARE
MANAGEMENT SERVICES ORGANIZATION

What is HIPAA?

- HIPAA is the Health Insurance Portability and Accountability Act of 1996.
- HIPAA is a Federal Law.
- HIPAA is a response, by Congress, to healthcare reform.
- HIPAA affects the health care industry.
- HIPAA is mandatory.

- Protects the privacy and security of PHI.
- Provides for electronic and physical security of PHI.
- Prevents health care fraud and abuse.
- Simplifies billing and other transactions, reducing health care administrative costs.

PROCARE
MANAGEMENT SERVICES ORGANIZATION

Who Must Follow the HIPAA Law?

Covered Entity

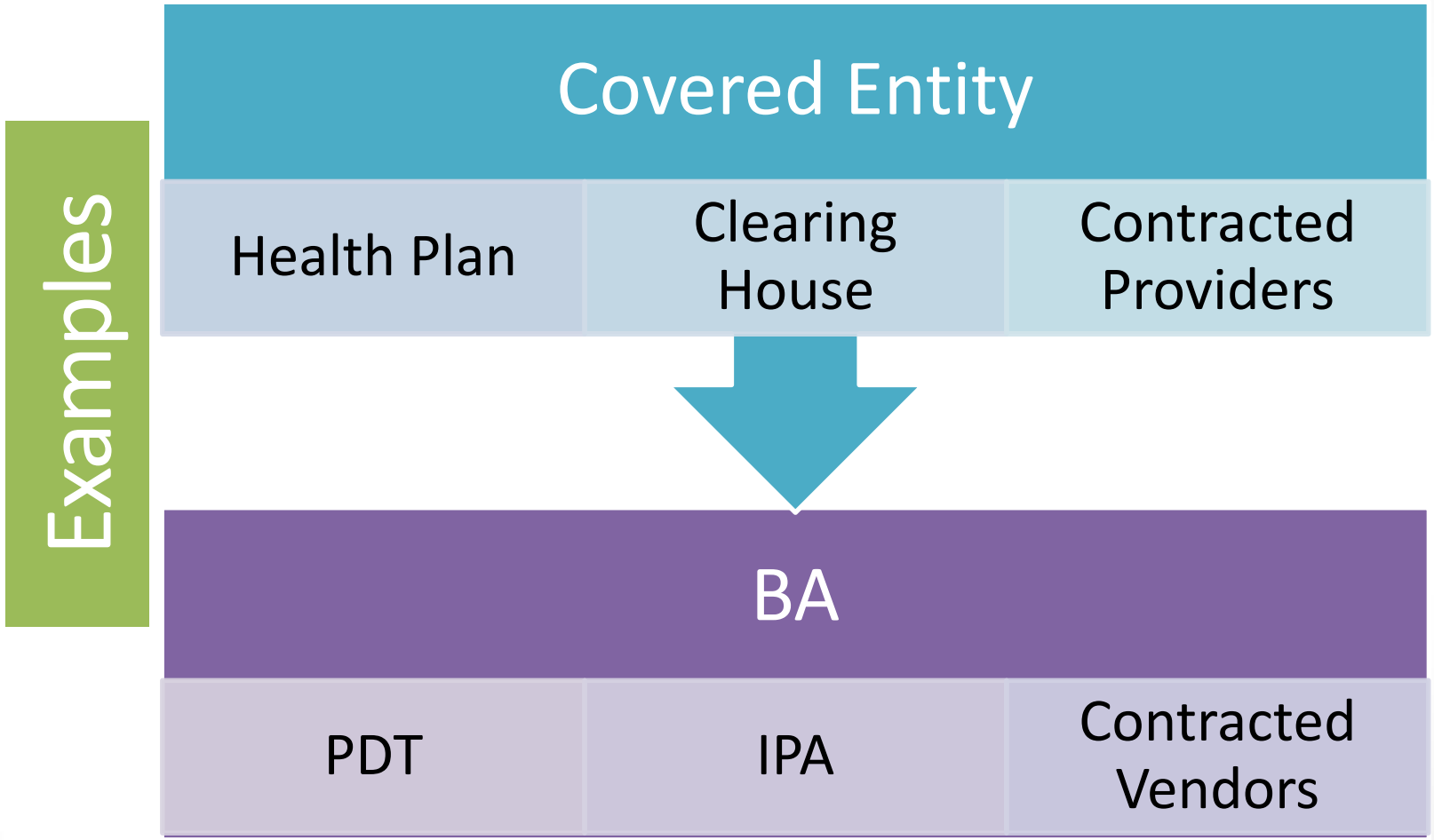
- HIPAA defines 3 categories of Covered Entities:
  - The Health Plan;
  - Health Care Clearinghouse;
  - Healthcare Providers; and all employees and departments that provide management, administrative, financial, legal, and operational support services to the extent that such employees and departments use and disclose individually identifiable health information.

Business Associate (BA)

- A person or entity which performs certain functions, activities, or services for or to a covered entity involving the use and/or disclosure of PHI, but the person or entity is not a part of the covered entity or its workforce.
- PDT and the IPAs are Business Associates and have agreements with Covered Entities (health plans and providers) to protect a patient's PHI.

PROCARE
MANAGEMENT SERVICES ORGANIZATION

Who Must Follow the HIPAA Law?



PROCARE
MANAGEMENT SERVICES ORGANIZATION

Who Must Follow the HIPAA Law?

Under HIPAA, the Covered Entity is responsible for all Protected Health Information (PHI), whether it is **transmitted**

- Electronically
- Paper Format
- Orally

Covered **transactions** include, but are not limited to

- Enrollment and dis-enrollment
- Premium payments
- Eligibility
- Referrals and Authorization
- Health Claims
- Health Care Payment and Remittance Advice

PROCARE
MANAGEMENT SERVICES ORGANIZATION

What is Considered PHI?

Protected Health Information (PHI)

- Relates to past, present, or future physical or mental conditions of an individual; provisions of healthcare to an individual; or for payment of care provided to an individual.
- Is transmitted or maintained in any form (electronic, paper, or oral representation.)
- Identifies, or can be used to identify the individual.

PROCARE
MANAGEMENT SERVICES ORGANIZATION

What is Considered PHI?

Examples of PHI (Health Information with Identifiers)

Name	Address (including street, city, zip, etc.)	Name of Employer
Any Date (birth, admit date, discharge date)	Telephone & Fax Numbers	E-mail Address
Social Security Number	Medical Records	Member ID Number

How Does HIPAA Affect PDT?

We are a business associate to covered entities, so **we may NOT…**

- Use/disclose an individual's PHI except as otherwise permitted or required by law.

But, we **may** use/disclose an individual's PHI for…

- Treatment of the Patient
- Payment of Healthcare Bills
- Business & Management Operations
- Disclosures Required by Law
- Public Health & Other Governmental Reporting

How Does HIPAA Affect PDT?

Treatment includes:

- Direct Patient Care
- Coordination of Care
- Consultations
- Referrals to Other Healthcare Providers

Payment includes:

- Any activity required to bill and collect for healthcare services provided to patients.

PROCARE
MANAGEMENT SERVICES ORGANIZATION

How Does HIPAA Affect PDT?

Healthcare Operations includes:

- Business Management
- Administrative Activities
- Quality Improvement
- Compliance
- Competency
- Training

PROCARE
MANAGEMENT SERVICES ORGANIZATION

How Does HIPAA Affect PDT?

We must use or share only the minimum amount of PHI necessary, except for requests made

- For treatment of the patient
- By the patient, or as requested by the patient to others
- By the Secretary of the Department of Health & Human Services (DHHS)
- As required by law
- To complete standardized electronic transactions, as required by HIPAA

PROCARE
MANAGEMENT SERVICES ORGANIZATION

How Does HIPAA Affect PDT?

For other uses or disclosures:

We must get signed authorization

from the patient.

Authorization must

- ❑ Describe the PHI to be used or released
- ❑ Identify who may use or release the PHI
- ❑ Identify who may receive the PHI
- ❑ Describe the purposes of the use or disclosure
- ❑ Identify when the authorization expires
- ❑ Be signed by the patient or someone making health care decisions (personal representative) for the patient

PROCARE MANAGEMENT SERVICES ORGANIZATION

How Does HIPAA Affect PDT?

The Covered Entity is required to:

- Give each patient a Notice of Privacy Practices that describes:
  - How the entity can use and share the patient's PHI
  - The patient's privacy rights
- Request every patient to sign a written acknowledgement that he/she has received the Notice of Privacy Practices.
- This typically happens at the provider level.

PROCARE
MANAGEMENT SERVICES ORGANIZATION

How Does HIPAA Affect PDT?

Notice of Privacy Practices explains what the covered entity is authorized to do with PHI.

Patient Privacy Rights include:

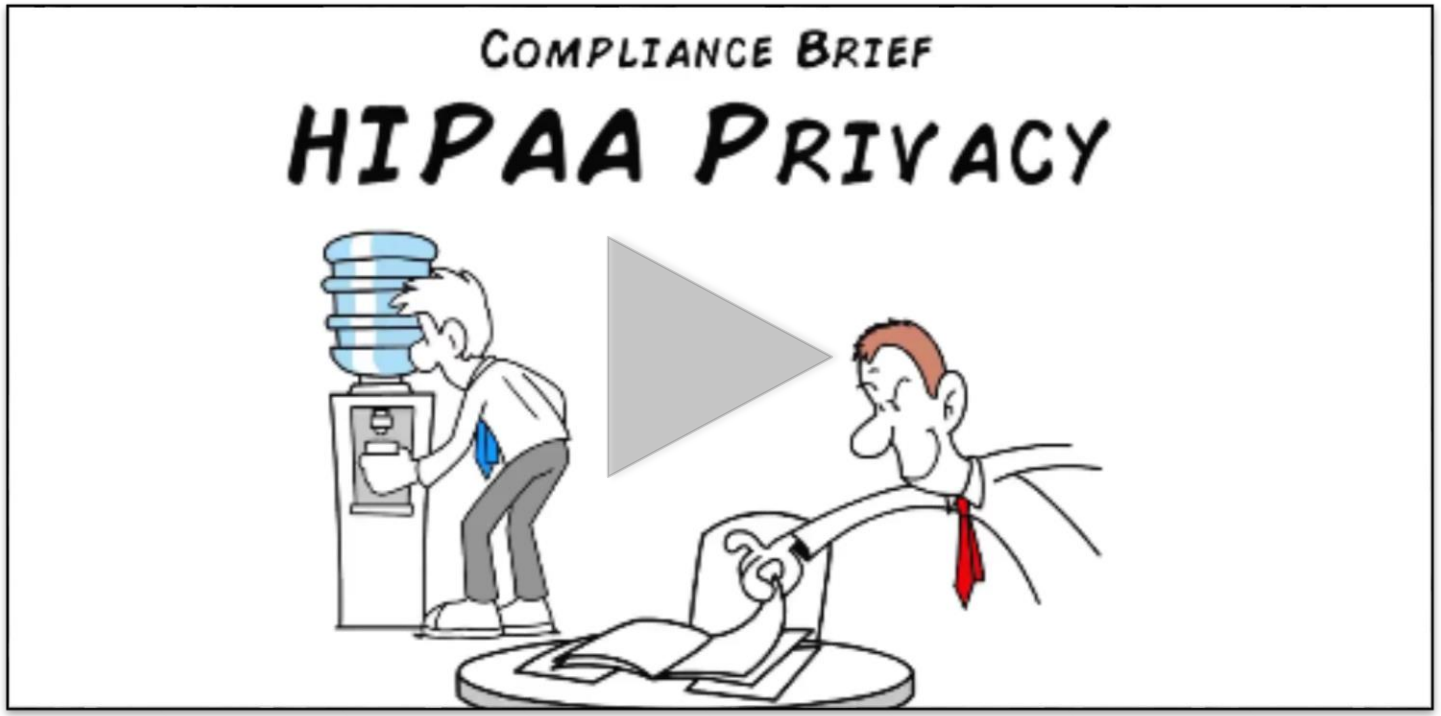
- The right to request restriction of PHI uses/disclosures
- The right to request alternative forms of communications (mail to P.O. Box, not street address; no message on answering machine, etc.)
- The right to access and copy patient's PHI
- The right to an accounting of the disclosures of PHI
- The right to request amendments to information

PROCARE
MANAGEMENT SERVICES ORGANIZATION

What Does this Mean to Me?

It is your job to

protect the privacy of the patient's PHI



Only access PHI required to do your job!

PROCARE
MANAGEMENT SERVICES ORGANIZATION

What are Some Other Uses & Disclosures?

Research

- PDT may not authorize the use or disclosure of PHI for research purposes except:
  - If the information is completely “de-identified.”
  - If the information is partially de-identified into a “limited data set” and the recipient of the information signs a data use agreement to protect the privacy of such information.
  - If PDT has obtained valid authorization from the individual subject of the information
  - If the Institutional Review Board, IRB, approves a waiver of the individual authorization requirement

What are Some Other Uses & Disclosures?

Marketing

A healthcare provider may use PHI to…

- Communicate to the patient about a health-related product or service that PDT provides.
- Communicate to the patient about general health issues: disease prevention, wellness classes, etc.

For all other marketing, patient authorization must be obtained, unless the communication is in the form of…

- Face-to-face communication made by the provider to an individual
- A promotional gift of nominal value provided by PDT

PROCARE MANAGEMENT SERVICES ORGANIZATION

How Do We Protect PHI?

<u>Avoid (unless it is required for your job)</u>

- Downloading, copying, or removing any PHI.
- Faxing information containing
  - Drug/Alcohol Dependency
  - Mental Illness or Psychological Information
  - Sexually-Transmitted Disease (STD) Information
  - HIV Status
- Including PHI in the subject line of electronic communication. (No exception)

Remember to return all copies of PHI upon termination or restriction of access to PHI.

PROCARE
MANAGEMENT SERVICES ORGANIZATION

How Do We Protect PHI?

Always

- Include a cover sheet containing a Confidentiality Statement when faxing.
- Limit faxing to when information is needed immediately for patient care or other situations considered urgent.
- Ensure you are faxing from a secure fax machine that is not accessible to the public.
- Notify the Compliance Officer if information is inadvertently faxed to a patient-restricted party or a recipient where there is a risk of release of the PHI (e.g., newspaper)

PROCARE
MANAGEMENT SERVICES ORGANIZATION

Privacy Scenario 1

Scenarios

Everyone in the Delegated Claims departments impacts members and providers. Review the following three scenarios that resulted in privacy incidents.

Eric Trusted the System

Member: Mrs. Zoe Tims

Claims employee: Eric

What happened? Zoe was inpatient at St. Vincent hospital from May 21 – June 2, 2016 when she passed away.

Upon receipt of the claim, the system attached the wrong provider. When processing the claim, the standard operating procedures indicated data entry verification was necessary. Eric trusted the system and did not verify data entry.

Impact: Zoe's PHI and payment for the claim went to the wrong provider. Payment to the correct provider was delayed.

What should have happened? Eric should have followed the standard operating procedures direction and verified data entry. When he became aware of the incident, he should report the incident.

Adopted from UHC M&R 2017 Privacy Incidents for delegated Claims

PROCARE MANAGEMENT SERVICES ORGANIZATION

Privacy Scenario 2

Tanisha Was Distracted

Member: Mr. Jose Torres

Claims employee: Tanisha

What happened? Jose suffered a contusion to his right knee and went to the emergency room. Tanisha is efficient and her fingers flew over the keys as she processed Jose's claim.

While verifying data entry, Tanisha determines the system attached the wrong provider. She updated the provider number, but keyed the number incorrectly, was distracted, and did not see her error.

Impact: Jose's PHI and payment for the claim went to the wrong provider. Payment to the correct provider was delayed.

What should have happened? Tanisha should pay close attention to her work and check for accuracy. When she became aware of the incident, she should report the incident.

Adopted from UHC M&R 2017 Privacy Incidents for delegated Claims

PROCARE MANAGEMENT SERVICES ORGANIZATION

Privacy Scenario 3

Joan Received John's Mail
Member: Mr. John Baker

Claims employee: Olivia

What happened? Joan Baker called in to say she received an Explanation of Benefits (EOB) for someone named John Baker. She has no idea who this person is…and there is PHI on the EOB.

When Olivia processed John's claim, she selected the wrong member (Joan) during member selection.

Impact: John's PHI was inappropriately shared with Joan.

What should have happened? Olivia should carefully follow processes and pay attention to detail to avoid mistakes. The Customer Service Representative that took the call should report this incident.

Adopted from UHC M&R 2017 Privacy Incidents for delegated Claims

PROCARE
MANAGEMENT SERVICES ORGANIZATION

Compliance Training

- ✓ Section 1: HIPAA Privacy
- ❑ Section 2: HIPAA Security
- ❑ Section 3: HITECH
- ❑ Section 4: Reporting a Breach
- ❑ Section 5: Disciplinary Actions
- ❑ Section 6: PDT Obligations & Resources

PROCARE
MANAGEMENT SERVICES ORGANIZATION

Section 2:
HIPAA Security Training

PROCARE
MANAGEMENT SERVICES ORGANIZATION

Security: Safeguarding e-PHI

- What is e-PHI and how do we protect it?
- Safeguard Best Practices
  - Access Controls
  - E-Mail Encryption
  - Workstation Security
  - Malware
  - Acceptable Computer Use
  - Data Management & Security
- Reminders

PROCARE
MANAGEMENT SERVICES ORGANIZATION

What is e-PHI & How to Protect it?

Electronic Protected Health Information (e-PHI)

Computer-based patient health information that is used, created, stored, received, or transmitted using any type of electronic information resource.

This includes

- Information in an electronic medical record
- Patient billing information transmitted to a payer
- Digital images and print outs
- Information when it is being sent by PDT to a provider, payer, or researcher

PROCARE
MANAGEMENT SERVICES ORGANIZATION

What is e-PHI & How to Protect it?

We must maintain security of e-PHI by ensuring the *confidentiality*, *integrity*, and *availability* of information through safeguards.

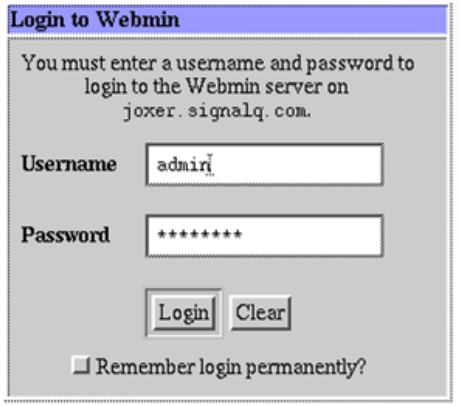
- *Confidentiality:* Ensure the information will not be disclosed without authorization.
- *Integrity:* Ensure the condition of information has not been altered or destroyed in an unauthorized manner and data is accurately transferred from one system to another.
- *Availability:* Ensure information is accessible and usable upon demand by authorized personnel.

PROCARE
MANAGEMENT SERVICES ORGANIZATION

Safeguards: Access Controls

Unique User Identifiers

Users are assigned a unique "User ID" for log-in purposes limiting access to the minimum required for the job.



- Never use anyone else's login or a computer when someone else is logged-on.
- Use of systems is audited for inappropriate access or use.
- Access is cancelled for terminated employees.

PROCARE MANAGEMENT SERVICES ORGANIZATION

Safeguards: Access Controls

Password Protection

- Passwords should be changed at least once every 6 months, or immediately after a breach.
- Each system should have a unique password.
- Passwords should not be inserted into E-mail messages or other forms of electronic communication.
- Personal Computers and other portable devices containing e-PHI must be password protected, and e-PHI encrypted.

PROCARE
MANAGEMENT SERVICES ORGANIZATION

Safeguards: Access Controls

Password Protection

- Default vendor passwords should be changed immediately.
- If you think someone has accessed your account, notify the Help Desk and your manager, and change your password IMMEDIATELY
- You are responsible for everything that occurs under your login.

PROCARE
MANAGEMENT SERVICES ORGANIZATION

Safeguards: E-mail Encryption

- By default, E-mail within our exchange server is encrypted with SSL.
- E-mail sent outside our domain (pdtrust.com) must have zsecure in the subject line.
- E-mail Encryption works only with “zsecure” in the subject line
  - It can be lowercase, uppercase, or mix case
  - It can be anywhere in the subject line
- For Microsoft Outlook, you can set the message sensitivity to confidential.
- Never include PHI in the subject line of an email.

PROCARE
MANAGEMENT SERVICES ORGANIZATION

Safeguards: Workstation Security

Workstations: Include electronic computing devices, laptops or desktop computers, or other devices that perform similar functions, and electronic media stored in or near them.

Physical Security Measures include

- Disaster Controls
- Physical Access Controls
- Device and Media Controls

PROCARE
MANAGEMENT SERVICES ORGANIZATION

Safeguards: Workstation Security

Disaster Controls	Physical Access Controls	Device & Media Controls
Protect workstations from natural and environmental hazards	Log-off before leaving a workstation	Auto log-off when possible & appropriate
Locate equipment above ground level to protect against floods	Lock offices, windows, sensitive papers, laptops, etc.	Set automatic screen savers which activate after 5 minutes
Move workstations away from overhead sprinklers	Use encryption tools when physical securities are unavailable	
Use surge protectors	Maintain key control	

Safeguards: Workstation Security

Workstation Checklist

- ✓Internet Firewall
- ✓Anti-virus software (up-to-date)
- ✓Install computer software updates
- ✓Encrypt & password-protect portable devices (laptops, etc.)
- ✓Lock office, file cabinets, or laptops
- ✓Use auto log-off from programs
- ✓Use password-protected screensavers
- ✓Back up critical data & programs

PROCARE
MANAGEMENT SERVICES ORGANIZATION

Safeguards: Workstation Security

When you take it with you…

- Smart Phones
  - Don’t store e-PHI on Smart Phones
  - If you must, de-identify or encrypt and password-protect data
  - Back up original files
  - Synchronize with computers as often as practical
  - Delete all unnecessary e-PHI
  - Protect your device from loss or theft
  - Always use a password on your phone!

PROCARE
MANAGEMENT SERVICES ORGANIZATION

Safeguards: Workstation Security

When you take it with you…

- USB/Memory Stick
  - Don’t store e-PHI on memory sticks
  - If you must, either de-identify or encrypt the data
  - Delete unnecessary e-PHI
  - Protect devices from loss or damage

PROCARE
MANAGEMENT SERVICES ORGANIZATION

Safeguards: Malware

Malware Controls are measures taken to protect against any software that causes unintended results

Malwares include

- Viruses
- Worms
- Spyware
- Keystroke Loggers
- Remote Access Trojans

PROCARE
MANAGEMENT SERVICES ORGANIZATION

Safeguards: Malware

Viruses	Attaches to a program or file. Attempts to spread through system/network.	Prevented by antivirus software	Download by user
Worms	Spread via security holes from user to user	Prevented by keeping security updates installed	Installed without user action
Spyware	Monitors habits and reports them to marketing database. Can open ad windows.		Installed w/o user knowing during install of another program or browsing the internet
Keystroke Loggers	Software or hardware that logs every keystroke	Detected by antivirus or spyware programs	Hardware is physically installed between keyboard and computer
Remote Access Trojan	Remote users connect to your computer	Detected by most antivirus programs	Appear as useful software, but will do damage once installed

Safeguards: Malware

Signs of Malware include

- Reduced performance (your computer slows or “freezes”)
- Windows opening by themselves
- Missing data
- Slow network performance
- Unusual toolbars added to your web browser

Contact the Help Desk if you suspect that your computer has malware installed.

PROCARE
MANAGEMENT SERVICES ORGANIZATION

Safeguards: Malware

Signs of Suspicious E-mail

- Any E-mail you receive with an attachment
- Any E-mail from someone whose name you do not recognize
- Phishing: Attempt to defraud the receiver by posing as a legitimate company.

Contact the Help Desk if you suspect you have a suspicious E-mail.

PROCARE
MANAGEMENT SERVICES ORGANIZATION

Safeguards: Malware

Signs of a Tampered Account

- Your account is locked when you try to open it
- Your password isn't accepted
- You are missing data
- Your computer settings have mysteriously changed

Contact the Help Desk if you suspect your account has by tampered.

PROCARE
MANAGEMENT SERVICES ORGANIZATION

Safeguards: Acceptable Computer Use

- Each individual is responsible for any violations associated with his or her User ID
- Use of computer system must be consistent with PDT goals
- All computer equipment and electronic data created by it belongs to PDT
- All users must comply with all Federal/State laws, PDT rules and policies, terms of computing contracts, and software licensing rules
- Take reasonable precautions to avoid introducing computer malware to the network, and participate and cooperate with the protection of IT infrastructure.

PROCARE
MANAGEMENT SERVICES ORGANIZATION

Safeguards: Acceptable Computer Use

DO NOT

- Engage in any activity that jeopardizes the availability, performance, integrity, or security of the computer system
- Use computing resources wastefully
- Use IT resources for personal gain or commercial activities not related to your job
- Install, copy, or use any software in violation of licensing agreements, copyrights, or contracts
- Try to access the files or E-mail of others unless authorized by the owner
- Harass, intimidate, or threaten others through e-messages

PROCARE
MANAGEMENT SERVICES ORGANIZATION

Safeguards: Acceptable Computer Use

DO NOT

- Construct a false communication that appears to be from someone else
- Send or forward unsolicited E-mail to lists of people you don't know
- Send, forward, or reply to E-mail chain letters
- Send out "Reply to all" mass E-mailings
- Create or transmit offensive, obscene, or indecent images, data, or other material
- Re-transmit virus hoaxes

Engaging in these activities could result in disciplinary action up to, and including, loss of network access, termination of employment, and civil or criminal liability

PROCARE MANAGEMENT SERVICES ORGANIZATION

Safeguards: Data Management & Security

Data Storage on Portable Devices:

- Permanent copies of e-PHI should not be stored on portable equipment, such as laptop, smart phone, and memory sticks
- If necessary, temporary copies can be used on portable devices only while using the data and if encrypted to safeguard the data if the device is lost or stolen

Data Disposal

- Destroy all e-PHI data which is no longer needed
- Know where to take hard drives, CDs, zip disks, or any backup devices for appropriate safe disposal or recycling

PROCARE
MANAGEMENT SERVICES ORGANIZATION

Security Reminders

A good security standard to follow is the "90 / 10" Rule:

- 10% of security safeguards are technical
- 90% of security safeguards rely on the user ("YOU") to adhere to good computing practices

Example: The lock on the door is the 10%. Your responsibility is 90%: Remembering to lock the door, checking to see if it is closed, ensuring others do not prop the door open, keeping control of keys.

10% security is worthless without YOU!

- Password protect your computers and devices
- Backup your e-PHI
- Keep offices secured
- Keep portable storage locked up
- Encrypt your e-PHI, if applicable

Compliance Training

- ✓ Section 1: HIPAA Privacy
- ✓ Section 2: HIPAA Security
- ❑ Section 3: HITECH
- ❑ Section 4: Reporting a Breach
- ❑ Section 5: Disciplinary Actions
- ❑ Section 6: PDT Obligations & Resources

PROCARE
MANAGEMENT SERVICES ORGANIZATION

Section 3: HITECH

PROCARE
MANAGEMENT SERVICES ORGANIZATION

HITECH

- What is HITECH?
- What Does HITECH Change?
- What is an Incident?
- What Constitutes a Breach?
- What Does the Law Cover?
- What Breach Exceptions Exist?
- What are PDT's Breach Notification Obligations?

PROCARE
MANAGEMENT SERVICES ORGANIZATION

What is HITECH?

- Health Information Technology for Economic & Clinical Health Act
- HITECH is a part of the American Recovery and Reinvestment Act of 2009
- It is a federal law that affects the healthcare industry
- Act allocated nearly $20 billion to health information technology projects, expanded the reach of HIPAA by extending certain obligations to business associates, and imposed a nationwide security breach notification law

PROCARE
MANAGEMENT SERVICES ORGANIZATION

What Does HITECH Change?

- Inclusion of a federal breach notification law for health information
  - Many states, including California, have data breach laws that require entities to notify individuals
  - State laws typically only pertain to personal information (which does not necessarily include medical information)
- The law requires covered entities and business associates to notify individuals, the Secretary of Health and Human Services, and, in some cases, the media in the event of a breach of unsecured PHI

PROCARE
MANAGEMENT SERVICES ORGANIZATION

What is an Incident?

Under HIPAA's Final Security Rule a "Security Incident" is

"The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.'' [45 CFR 164.304]

PROCARE
MANAGEMENT SERVICES ORGANIZATION

What is a Breach?

A “Security Breach” is impermissible acquisition, access, use, or disclosure not permitted by the HIPAA Privacy Rule.

Examples include

- Laptop containing PHI is stolen
- Receptionist who is not authorized to access PHI looks through patient files in order to learn of a person’s treatment
- Nurse gives discharge papers to the wrong individual
- Billing statements containing PHI are mailed or faxed to the wrong individual/entity

PROCARE
MANAGEMENT SERVICES ORGANIZATION

What is a Breach?

For an incident to be a breach it must…

- Pose significant risk of financial, reputational, or other harm to the individual whose PHI was used or disclosed.
  - For example) If disclosed PHI included the name of an individual and the fact that he received services from a hospital, then this would constitute a violation of the Privacy Rule, but it may not constitute a significant risk of financial or reputational harm to the individual.
  - If the information includes PHI that increases the risk of identity theft (such as a social security number or date of birth) then there is a higher risk of impermissible use or disclosure.
- We are responsible for conducting a risk assessment that should be fact specific.

PROCARE
MANAGEMENT SERVICES ORGANIZATION

What Breach Exceptions Exist?

Exceptions include unintentional acquisition, access, use, or disclosure by a workforce member acting under the authority of a covered entity or business associate

- Workforce members are "employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity"
- Example) Bill, a billing employee, receives and opens an e-mail containing PHI not intended for him. Bill notices he is not the intended recipient, alerts the sender of the e-mail, and then deletes it. Bill unintentionally accessed unauthorized PHI. However, the use of information was done in good faith and within the scope of authority, and therefore, does not constitute a breach.

What Breach Exceptions Exist?

Exceptions include inadvertent disclosures of PHI from a person authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the same covered entity, business associate, or organized healthcare arrangement in which covered entity participates.

- Organized health care arrangement means, among other things, a clinically integrated care setting in which individuals typically receive health care from more than one health care provider such as a hospitals and the health care providers who have staff privileges at the hospital.

PROCARE
MANAGEMENT SERVICES ORGANIZATION

What Breach Exceptions Exist?

If a covered entity or business associate has a good faith belief that the unauthorized individual, to whom the impermissible disclosure was made, would not have been able to retain the information.

- Example) EOBs are sent to the wrong individuals. A few of them are returned by the post office unopened as undeliverable. It could be concluded that the improper addresses could not have reasonably retained the information. The EOBs that were not returned as undeliverable however, and that the covered entity knows were sent to the wrong individuals, should be treated as potential breaches.

PROCARE
MANAGEMENT SERVICES ORGANIZATION

What Does the Law Cover?

HITECH applies to breaches of unsecure PHI

- Remember PHI, Protected Health Information, is health information with identifiers.
- Information must be encrypted or destroyed in order to be considered “secured.”
- PHI can relate to past, present, or future physical or mental conditions, provision of healthcare, or payment of care.
- This includes PHI transmitted or maintained in any form (electronic, paper, or oral representation).

PROCARE
MANAGEMENT SERVICES ORGANIZATION

Breach Notification Obligations

Following a breach, PDT is responsible for providing notice to

- The affected individuals: Without unreasonable delay and in no event later than 60 days from the date of discovery.
  - A breach is considered discovered when the incident becomes known, not when the covered entity or Business Associate concludes the analysis of whether the facts constitute a breach.
- Secretary of Health & Human Services (HHS): Timing depends on number of individuals affected.
- Media: Only required if 500 or more individuals of any one state are affected.

PROCARE
MANAGEMENT SERVICES ORGANIZATION

Compliance Training

- ✓ Section 1: HIPAA Privacy
- ✓ Section 2: HIPAA Security
- ✓ Section 3: HITECH
- ❑ Section 4: Reporting a Breach
- ❑ Section 5: Disciplinary Actions
- ❑ Section 6: PDT Obligations & Resources

PROCARE
MANAGEMENT SERVICES ORGANIZATION

Section 4:
Reporting a Breach

PROCARE
MANAGEMENT SERVICES ORGANIZATION

Reporting a Breach

- What is Your Responsibility?
- What if a Breach is Reported?
- The Decision Tree for Breach Notification

PROCARE
MANAGEMENT SERVICES ORGANIZATION

What is Your Responsibility?

All workforce members must be trained to ensure they are aware of the importance of timely reporting of privacy and security incidents and of the consequences of failing to do so.

If you notice a breach of Confidentiality, Security, or Policy and Procedure, **you are required to respond to and report the incident/breach to the PDT Compliance Officer:**

Karen Palmer, CHC
(562) 860-8771 x114
compliance@pdtrust.com

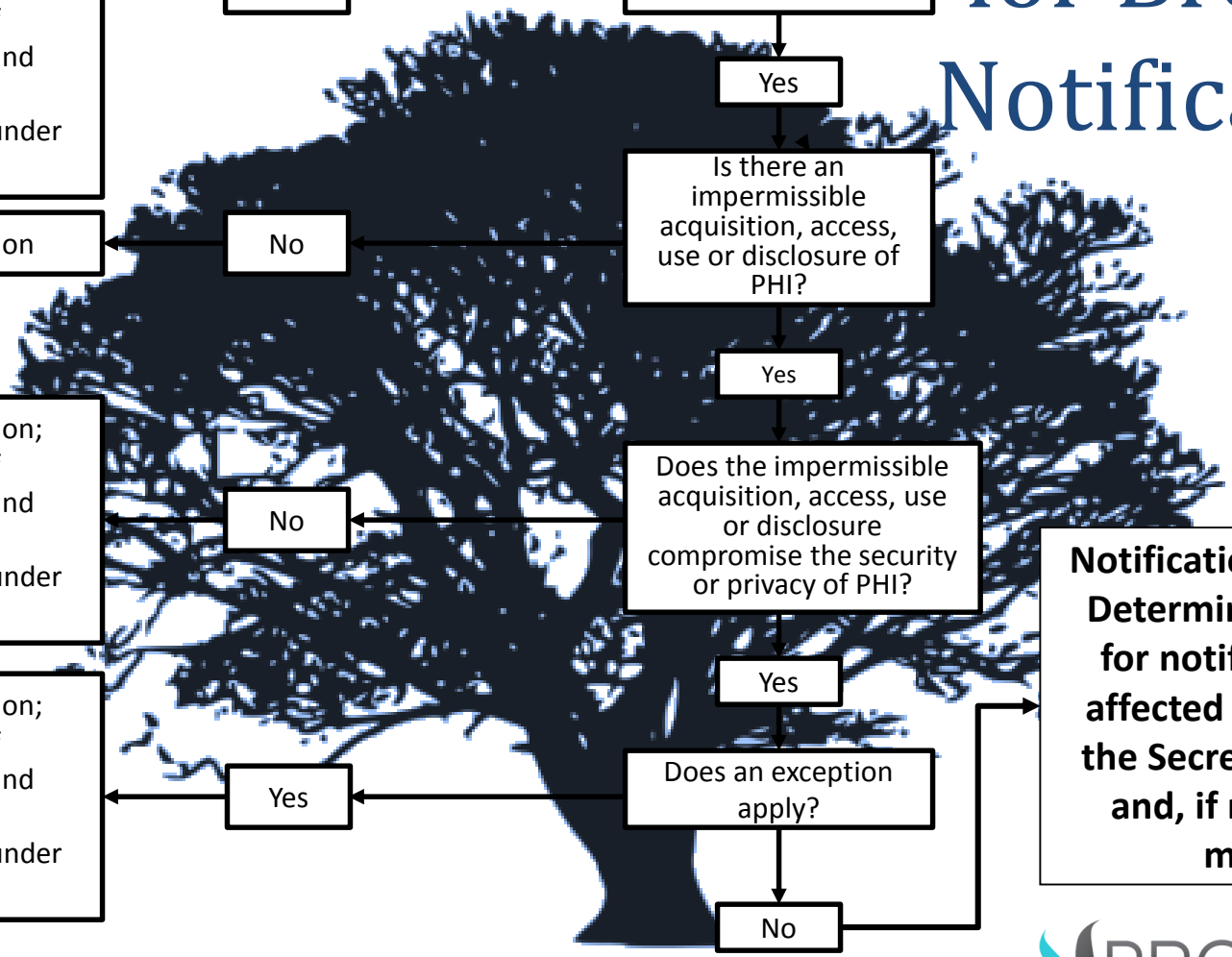
PROCARE
MANAGEMENT SERVICES ORGANIZATION

What if a Breach is Reported?

- The incident will be thoroughly investigated.
- We are required to attempt to remedy the harmful effects of any breach.
  - This includes providing notification to affected individuals.

PROCARE
MANAGEMENT SERVICES ORGANIZATION

Decision Tree for Breach Notification



Is the information PHI?

- No → No Notification; Determine if Red Flag Rules or state breach notification laws apply
- Yes ↓

Is the PHI unsecured?

- No → No Notification; Determine if accounting and mitigation obligations under HIPAA
- Yes ↓

Is there an impermissible acquisition, access, use or disclosure of PHI?

- No → No Notification
- Yes ↓

Does the impermissible acquisition, access, use or disclosure compromise the security or privacy of PHI?

- No → No Notification; Determine if accounting and mitigation obligations under HIPAA
- Yes ↓

Does an exception apply?

- Yes → No Notification; Determine if accounting and mitigation obligations under HIPAA
- No ↓

Notification Required; Determine methods for notification for affected individuals, the Secretary of HHS and, if necessary, media

PROCARE MANAGEMENT SERVICES ORGANIZATION

Compliance Training

- ✓ Section 1: HIPAA Privacy
- ✓ Section 2: HIPAA Security
- ✓ Section 3: HITECH
- ✓ Section 4: Reporting a Breach
- ❑ Section 5: Disciplinary Actions
- ❑ Section 6: PDT Obligations & Resources

PROCARE
MANAGEMENT SERVICES ORGANIZATION

Section 5: Disciplinary Actions

PROCARE
MANAGEMENT SERVICES ORGANIZATION

Disciplinary Actions

- Disciplinary Actions
  - Internal
  - Civil
- Sanctions
- Civil Penalties

PROCARE
MANAGEMENT SERVICES ORGANIZATION

Disciplinary Actions

Internal Disciplinary Actions

- Individuals who breach the policies will be subject to appropriate discipline.

Civil Penalties

- Covered entities and individuals who violate these standards will be subject to civil liability.

An employee who does not protect a patient's privacy or does not report a breach, HIPAA incident, or FWA incident in accordance with PDT policies and procedures could lose his or her job!

PROCARE
MANAGEMENT SERVICES ORGANIZATION

Sanctions

Level & Definition of Violation	Action	Example
Accidental and/or due to lack of proper education	• Re-training and re-evaluation • Oral warning with documented discussions of policy, procedures, and requirements	• Improper disposal of PHI. • Improper protection of PHI (leaving records on counters, leaving documents in inappropriate areas). • Not properly verifying individuals.
Purposeful violation of privacy or an unacceptable number of previous violations	• Re-training and re-evaluation • Written warning with discussion of policy, procedures, and requirements	• Accessing or using PHI without have a legitimate need • Not forwarding appropriate information or requests to the privacy official for processing
Purposeful violation of privacy policy with associated potential for patient harm	Termination	• Disclosure of PHI to unauthorized individual or company • Not reporting FWA • Sale of PHI to any source • Any uses or disclosures that could invoke harm to a patient

Civil Penalties

- $100 per violation
- $25,000 for an identical violation within one year
- $50,000 for wrongful disclosure
- $100,000 and/or 5 years in prison for wrongful violation for obtaining PHI under false pretenses
- $250,000 and/or 10 years in prison if the individual committed the breach with intent to sell or transfer PHI for commercial advantage, personal gain, or malicious harm, includes obtaining or disclosing

PROCARE
MANAGEMENT SERVICES ORGANIZATION

Civil Penalties

Circumstance of Violation	Minimum Penalty	Maximum Penalty
Entity did not know (even with reasonable diligence)	$100 per violation ($25,000 per year for violating same requirement)	$50,000 per violation ($1.5 million annually)
Reasonable cause, not willful neglect	$1,000 ($100,000)	$50,000 ($1.5 million)
Willful neglect, but corrected within 30 days	$10,000 ($250,000)	$50,000 ($1.5 million)
Willful neglect, not corrected	$50,000 ($1.5 million)	None

PROCARE
MANAGEMENT SERVICES ORGANIZATION

Compliance Training

- ✓ Section 1: HIPAA Privacy
- ✓ Section 2: HIPAA Security
- ✓ Section 3: HITECH
- ✓ Section 4: Reporting a Breach
- ✓ Section 5: Disciplinary Actions
- ❑ Section 6: PDT Obligations & Resources

PROCARE
MANAGEMENT SERVICES ORGANIZATION

Section 6:
PDT Obligation & Resources

PROCARE
MANAGEMENT SERVICES ORGANIZATION

Employee Obligations

- Do not disclose PHI without patient authorization.
  - If you have questions about whether a disclosure is permitted, ask your supervisor.
- If you think there has been an unauthorized disclosure of PHI, contact the Compliance Officer.
- When removing PHI from our office (physical or electronic,) act in accordance with our security measures.

PROCARE
MANAGEMENT SERVICES ORGANIZATION

HIPAA Policies and Procedures

For PDT employees, all policies are located on the PDT HR & Compliance folder on the PDT desktop.

- PDT HR & Compliance\HR Resource\Compliance\P&Ps

For external parties, please submit a request to PDT's Compliance Officer or your Provider Relations contact.

PROCARE
MANAGEMENT SERVICES ORGANIZATION

Compliance Contact

Physicians DataTrust Compliance Officer

Karen Palmer, CHC

(562) 860-8771 x114

compliance@pdtrust.com

17215 Studebaker Rd, Ste 320

Cerritos, CA 90703

PROCARE
MANAGEMENT SERVICES ORGANIZATION

Thank You!

For more information about HIPAA, visit https://www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/HIPAAGenInfo/index.html?redirect=/hipaageninfo/

PROCARE
MANAGEMENT SERVICES ORGANIZATION