



IMPERIAL COUNTY  
**Behavioral Health Services**  
MENTAL HEALTH & SUBSTANCE USE RECOVERY

# HIPAA PRIVACY & SECURITY TRAINING

2024

1

1

## TRAINING OBJECTIVES

- ▶ Understand what HIPAA IS
- ▶ Learn the purpose of HIPAA
- ▶ Understand key HIPAA terms
- ▶ Understand what information must be protected and how it can be protected
- ▶ Expectations of ICBHS employees and volunteers
- ▶ Learn the penalties for noncompliance with HIPAA regulations
- ▶ Provide instructions to report a possible privacy breach

2

2

## HIPAA OVERVIEW



3

3

## WHAT IS “HIPAA”?

HIPAA is an acronym for:

**H**health  
**I**nsurance  
**P**ortability (and)  
**A**ccountability  
**A**ct



4

4

## WHAT IS HIPAA?

To improve the efficiency and effectiveness of the health care system, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) included Administrative Simplification provisions that required the US Department of Health and Human Services (HHS) to adopt national standards for electronic health care transactions and code sets, unique health identifiers, and security.

At the same time, Congress recognized that advances in electronic technology could erode the privacy of health information. Consequently, Congress incorporated into HIPAA provisions that mandated the adoption of Federal privacy protections for individually identifiable health information.

5

5

## WHAT IS HIPAA?

- HHS published a final Privacy Rule in December 2000, which was later modified in August 2002. This Rule set national standards for the protection of individually identifiable health information by three types of covered entities: health plans, health care clearinghouses, and health care providers who conduct the standard health care transactions electronically.
- HHS published a final Security Rule in February 2003. This Rule sets national standards for protecting the confidentiality, integrity, and availability of electronic protected health information.
- The Enforcement Rule provides standards for the enforcement of HIPAA standards.
- HHS enacted a final Omnibus rule that implements a number of provisions of the HITECH Act to strengthen the privacy and security protections for health information established under HIPAA, finalizing the Breach Notification Rule.

6

6

# THE PRIVACY RULE



7

7

## THE PRIVACY RULE - INTRODUCTION

The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other individually identifiable health information (collectively defined as "protected health information"). The Privacy Rule requires appropriate safeguards to protect the privacy of protected health information and sets limits and conditions on the uses and disclosures that may be made of such information without an individual's authorization.

The Privacy Rule also gives individuals rights over their protected health information, including rights to examine and obtain a copy of their health records, to direct a covered entity to transmit to a third party an electronic copy of their protected health information in an electronic health record, and to request corrections.

8

8

## WHO IS COVERED BY THE PRIVACY RULE?

The Privacy Rule applies to two groups:

### 1. Covered Entities

- ▶ *Health Plans* – individual and group plans that provide or pay the cost of medical care.
- ▶ *Health Care Providers* – anyone who provides medical care and electronically transmits health information in the provision of that care (i.e. submits claims for reimbursement).
- ▶ *Clearinghouses* – entities such as those that provide billing services or community health management information systems.

9

HIPAA - The Privacy Rule

9

## WHO IS COVERED BY THE PRIVACY RULE?

The Privacy Rule applies to two groups:

### 2. Business Associates

- ▶ A person or organization that performs certain functions, activities, or services for or to ICBHS which involves the use and/or disclosure of protected health information but that person or organization is not part of the ICBHS workforce.
- ▶ Business Associates are required to sign a Business Associate Agreement before providing services for ICBHS.
- ▶ Anyone who is not employed by ICBHS but has access to protected health information of ICBHS patients is considered a Business Associate.

10

HIPAA - The Privacy Rule

10

## WHAT INFORMATION IS PROTECTED BY THE PRIVACY RULE?

The Privacy Rule protects all "*individually identifiable health information*" held or transmitted by a covered entity or its business associate, in any form or media, whether **electronic, paper, or oral**. The Privacy Rule calls this information "protected health information" or PHI.

11

HIPAA - The Privacy Rule

11

## WHAT INFORMATION IS PROTECTED BY THE PRIVACY RULE?

"Individually identifiable health information" is information, including demographic data, that relates to:

- ▶ The individual's past, present or future physical or mental health condition,
- ▶ The provision of health care to the individual, or
- ▶ The past, present, or future payment for the provision of health care to the individual,
- ▶ AND that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual. Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number).

12

HIPAA - The Privacy Rule

12

# WHAT INFORMATION IS PROTECTED BY THE PRIVACY RULE?

## Components of identifiable information include:

- ▶ Name
- ▶ Address
- ▶ Certificate/License Number
- ▶ Elements of dates related to a patient, such as date of birth, admission date, or discharge date
- ▶ Telephone and/or fax number
- ▶ Social Security number
- ▶ Email Address
- ▶ Medical Record Number
- ▶ Health Plan Beneficiary Number
- ▶ Account Number (BC#)
- ▶ Any vehicle or device serial number, including license plate
- ▶ Web addresses (URLs)
- ▶ Internet Protocols (IP) Address
- ▶ Finger or voice prints
- ▶ Photographic images
- ▶ Age greater than 89 (as the 90 year old population is very small)
- ▶ Any other unique identifying number/characteristic/code

13

HIPAA - The Privacy Rule

13

# WHAT INFORMATION IS PROTECTED BY THE PRIVACY RULE?

Examples of PHI include:

- ▶ Patient medical records
- ▶ Bills from health care providers
- ▶ Information about health care services provided to patients
- ▶ Demographic information about a patient
- ▶ Provider appointment lists / daily schedules

14

HIPAA - The Privacy Rule

14

## POLL #1

15

15

## GENERAL PRINCIPLES FOR USES AND DISCLOSURES

A major purpose of the Privacy Rule is to define and limit the circumstances in which an individual's protected health information may be used or disclosed by covered entities.

A covered entity may not **use or disclose** PHI, **except as permitted or required**.

A covered entity must disclose PHI in only two situations:

1. To individuals (or their personal representatives) specifically when they request access to, or an accounting of disclosures of, their PHI; and,
2. To HHS when it is undertaking a compliance investigation or review or enforcement action.

16

16



## GENERAL PRINCIPLES FOR USES AND DISCLOSURES

- ▶ Information is used when we review or use PHI internally for:
  - ▶ Collecting information by clinical staff
  - ▶ Reviewing patient charts by Compliance or Quality Management
  - ▶ Completing billing forms by Fiscal
- ▶ Information is disclosed when we release or provide PHI to others:
  - ▶ Sending prescriptions to a pharmacy
  - ▶ Sending patient records to another provider
  - ▶ Updating a social worker on a patient's case

17

HIPAA - The Privacy Rule

17

## GENERAL PRINCIPLES FOR USES AND DISCLOSURES

The next set of slides will summarize HIPAA standards regarding the use and disclosure of PHI, but you may also review the following ICBHS policies and procedures for additional information:

- ▶ **Policy 01-22**, HIPAA-Authorization for the Use and Disclosure of Protected Health Information
- ▶ **Policy 01-64**, Revocation to Use or Disclose Protected Health Information
- ▶ **Procedure 01-05**, Release of Client Information
- ▶ **Procedure 01-11**, Authorization for the Use or Disclosure of Information Processing and Billing
- ▶ **Procedure 01-12**, Revocation of Authorization to Use or Disclose Protected Health Information
- ▶ **Procedure 01-17**, Confirming the Validity of an Authorization for the Release of Information

18

HIPAA - The Privacy Rule

18

## PERMITTED USES AND DISCLOSURES

A covered entity is permitted, but not required, to use and disclose PHI, *without an individual's authorization*, for the following purposes or situations:

1. To the Individual (unless required for access or accounting of disclosures);
2. Treatment, Payment, and Health Care Operations;
3. Opportunity to Agree or Object;
4. Incident to An Otherwise Permitted Use and Disclosure;
5. Public Interest and Benefit Activities; and,
6. Limited Data Set for the purposes of research, public health or health care operations.

Covered entities may rely on professional ethics and best judgments in deciding which of these permissive uses and disclosures to make.

19

HIPAA - The Privacy Rule

19

## PERMITTED USES AND DISCLOSURES

A covered entity is permitted, but not required, to use and disclose PHI, *without an individual's authorization*, for the following purposes or situations:

1. To the Individual.
  - ▶ A covered entity may disclose PHI to the individual who is the subject of the information.
    - ▶ Instances where a covered entity may decide not to disclose PHI to the individual include requests for psychotherapy notes or PHI that is compiled for legal proceedings, or when access to the information would endanger a person's life or safety.

20

HIPAA - The Privacy Rule

20

## PERMITTED USES AND DISCLOSURES

A covered entity is permitted, but not required, to use and disclose PHI, *without an individual's authorization*, for the following purposes or situations:

2. Treatment, Payment, and Health Care Operations.
  - ▶ **Treatment** is the provision, coordination, or management of health care and related services for an individual by one or more health care providers, including consultation between providers regarding a patient and referral of a patient by one provider to another.
  - ▶ **Payment** encompasses activities of a health plan to obtain premiums, determine or fulfill responsibilities for coverage and provision of benefits, and furnish or obtain reimbursement for health care delivered to an individual and activities of a health care provider to obtain payment or be reimbursed for the provision of health care to an individual.

21

HIPAA - The Privacy Rule

21

## PERMITTED USES AND DISCLOSURES

A covered entity is permitted, but not required, to use and disclose PHI, *without an individual's authorization*, for the following purposes or situations:

2. Treatment, Payment, and Health Care Operations.
  - ▶ **Health care operations** are any of the following activities:
    - ▶ Quality assessment and improvement activities, including case management and care coordination;
    - ▶ Competency assurance activities, including provider or health plan performance evaluation, credentialing, and accreditation;
    - ▶ Conducting or arranging for medical reviews, audits, or legal services, including fraud and abuse detection and compliance programs;
    - ▶ Specified insurance functions, such as underwriting, risk rating, and reinsuring risk;
    - ▶ Business planning, development, management, and administration; and,
    - ▶ Business management and general administrative activities of the entity, including but not limited to: de-identifying PHI, creating a limited data set, and certain fundraising for the benefit of the covered entity.

22

HIPAA - The Privacy Rule

22

## PERMITTED USES AND DISCLOSURES

A covered entity is permitted, but not required, to use and disclose PHI, *without an individual's authorization*, for the following purposes or situations:

### 2. Treatment, Payment, and Health Care Operations.

#### ▶ Examples include:

- ▶ A referring provider calls to request a copy of the intake assessment (Treatment)
- ▶ A patient's insurance company calls to request a copy of the progress note for a specific date of service (Payment)
- ▶ The Quality Management Unit conducts program chart reviews (Operations)

23

HIPAA - The Privacy Rule

23

## PERMITTED USES AND DISCLOSURES

A covered entity is permitted, but not required, to use and disclose PHI, *without an individual's authorization*, for the following purposes or situations:

### 3. Opportunity to Agree or Object.

- ▶ Informal permission may be obtained by asking the individual outright, or by circumstances that clearly give the individual the opportunity to agree, acquiesce, or object.
- ▶ Example: (1) facility directory of patient contact information maintained by a hospital. (2) when a pharmacist dispenses a filled prescription to a person acting on behalf of a patient.

24

HIPAA - The Privacy Rule

24

## PERMITTED USES AND DISCLOSURES

A covered entity is permitted, but not required, to use and disclose PHI, *without an individual's authorization*, for the following purposes or situations:

4. Incident to An Otherwise Permitted Use and Disclosure.
  - ▶ The Privacy Rule permits certain incidental uses and disclosures that occur as a by-product of another permissible or required use or disclosure, as long as the covered entity has applied reasonable safeguards and implemented the minimum necessary standard, where applicable, with respect to the primary use or disclosure.
  - ▶ An incidental use or disclosure is a secondary use or disclosure that cannot reasonably be prevented, is limited in nature, and that occurs as a result of another use or disclosure that is permitted by the Rule.
  - ▶ Example: a clinic visitor overhears a provider's confidential conversation with another provider or a patient.

25

HIPAA - The Privacy Rule

25

## PERMITTED USES AND DISCLOSURES

A covered entity is permitted, but not required, to use and disclose PHI, *without an individual's authorization*, for the following purposes or situations:

4. Incident to An Otherwise Permitted Use and Disclosure.
  - ▶ Reasonable safeguards for limiting incidental uses or disclosures include:
    - ▶ Speaking quietly when discussing a patient's condition with family members in a waiting room or other public area.
    - ▶ Avoiding using patients' names in public hallways and elevators, and posting signs to remind employees to protect patient confidentiality.

26

HIPAA - The Privacy Rule

26

## PERMITTED USES AND DISCLOSURES

A covered entity is permitted, but not required, to use and disclose PHI, *without an individual's authorization*, for the following purposes or situations:

5. Public Interest and Benefit Activities.
  - ▶ The Privacy Rule permits use and disclosure of PHI, without an individual's authorization or permission, for 12 national priority purposes. These disclosures are permitted, although not required, by the Privacy Rule in recognition of the important uses made of health information outside of the health care context.
  - ▶ Specific conditions or limitations apply to each public interest purpose, including additional restrictions placed by the state of California, so always ask your supervisor before disclosing any PHI.

27

HIPAA - The Privacy Rule

27

## PERMITTED USES AND DISCLOSURES

A covered entity is permitted, but not required, to use and disclose PHI, *without an individual's authorization*, for the following purposes or situations:

5. Public Interest and Benefit Activities. These include:
  - ▶ Those required by law;
  - ▶ Public health activities;
  - ▶ Victims of abuse, neglect, or domestic violence;
  - ▶ Health oversight activities;
  - ▶ Judicial and administrative proceedings;
  - ▶ Law enforcement purposes;

28

HIPAA - The Privacy Rule

28

## PERMITTED USES AND DISCLOSURES

A covered entity is permitted, but not required, to use and disclose PHI, *without an individual's authorization*, for the following purposes or situations:

5. Public Interest and Benefit Activities. These include:
  - ▶ Decedents;
  - ▶ Cadaveric organ, eye, or tissue donation;
  - ▶ Research;
  - ▶ Serious threat to health or safety;
  - ▶ Essential government functions; and,
  - ▶ Worker's Compensation.

29

HIPAA - The Privacy Rule

29

## PERMITTED USES AND DISCLOSURES

A covered entity is permitted, but not required, to use and disclose PHI, *without an individual's authorization*, for the following purposes or situations:

6. Limited Data Set for the purposes of research, public health or health care operations.
  - ▶ A limited data set is PHI from which certain specified direct identifiers of individuals and their relatives, household members, and employers have been removed. A limited data set may be used and disclosed for research, health care operations, and public health purposes, provided the recipient enters into a data use agreement promising specified safeguards for the PHI within the limited data set.

30

HIPAA - The Privacy Rule

30

## PERMITTED USES AND DISCLOSURES

Certain limitations and restrictions may apply to each permitted use and disclosure of PHI granted under HIPAA, including more stringent privacy laws within the state of California.

**Always** consult with your immediate supervisor or the Privacy Officer before you disclose any PHI without a signed release of information.

31

HIPAA - The Privacy Rule

31

POLL #2

32

32



## AUTHORIZED USES AND DISCLOSURES

- ▶ The individual's written authorization must be obtained for any use or disclosure of PHI that is not otherwise permitted or required by the Privacy Rule.
- ▶ Examples of disclosures that would require an individual's authorization include:
  - ▶ Disclosures to a school regarding group attendance for a student.
  - ▶ Disclosures to a family member regarding a patient's current treatment.
  - ▶ Disclosures to a lawyer for a patient's legal proceedings.
- ▶ **Written** authorization must be obtained **PRIOR** to use or disclosure.

33

HIPAA - The Privacy Rule

33

## AUTHORIZED USES AND DISCLOSURES

- ▶ The *required* elements of an authorization include:
  - ▶ Description of the PHI to be disclosed;
  - ▶ Name(s) of the person(s) authorized to make the request for use or disclosure;
  - ▶ Name(s) of person(s) who may use the PHI or to whom the covered entity may make the requested disclosure;
  - ▶ Description of each purpose of the requested use or disclosure;
  - ▶ Authorization expiration date or event that relates to the individual or to the purpose of the use or disclosure;

34

HIPAA - The Privacy Rule

34

## AUTHORIZED USES AND DISCLOSURES

- ▶ The *required* elements of an authorization include:
  - ▶ Signature of the individual and date; and,
    - ▶ If a personal representative signs, a description must be included of the representative's authority to act for the individual.
  - ▶ The following statements:
    - ▶ The patient has the right to revoke the authorization at any time (with certain exceptions) by submitting a written statement to the covered entity.
    - ▶ ICBHS generally may not condition treatment on the provision of the authorization.
    - ▶ The information disclosed per the authorization may be subject to re-disclosure and no longer protected.

\*Note that 42 CFR Part 2 places additional requirements upon the written consents utilized by SUD programs.

35

HIPAA - The Privacy Rule

35

## AUTHORIZED USES AND DISCLOSURES

- ▶ An authorization is not valid if:
  - ▶ The expiration date has passed
  - ▶ It is not filled out completely or correctly
  - ▶ It has been revoked by the patient
  - ▶ Any material information in the authorization is known to be false

See **ICBHS Policy 01-22** and **ICBHS Procedure 01-17**.

36

HIPAA - The Privacy Rule

36

## VERIFYING IDENTITY AND AUTHORITY

ICBHS staff and providers must verify the identity of any unknown person who requests PHI and verify the authority of any person who requests PHI. See **ICBHS Policy 01-78**.

This means:

- ▶ Confirming the identity of the person, if the person is not readily known; and,
- ▶ Verifying that the person is authorized to receive the PHI.

**ICBHS Procedure 01-16** provides guidance for verifying the identity and authority of any person requesting PHI.

37

HIPAA - The Privacy Rule

37

## When in doubt...

**Always** make sure you have a **written** authorization before disclosing PHI.

You can also ask your immediate supervisor or the ICBHS Privacy Officer if it's okay to release any PHI.

38

HIPAA - The Privacy Rule

38

# LIMITING USES AND DISCLOSURES TO THE MINIMUM NECESSARY

## Minimum Necessary

- ▶ A central aspect of the Privacy Rule is the principle of "minimum necessary" use and disclosure. A covered entity must make reasonable efforts to use, disclose, and request only the *minimum amount of PHI needed to accomplish the intended purpose of the use, disclosure, or request*. See **ICBHS Policy 01-72**.
- ▶ The minimum necessary requirement is not imposed in any of the following circumstances:
  - ▶ Disclosure to or a request by a health care provider for treatment;
  - ▶ Disclosure to an individual who is the subject of the information, or the individual's personal representative;
  - ▶ Use or disclosure made pursuant to an authorization;
  - ▶ Disclosure to HHS for complaint investigation, compliance review or enforcement;
  - ▶ Use or disclosure that is required by law; or,
  - ▶ Use or disclosure required for compliance with the HIPAA Transactions Rule or other HIPAA Administrative Simplification Rules.

39

HIPAA - The Privacy Rule

39

## POLL #3

40

40

## POLL #4

41

41

## INDIVIDUAL PRIVACY RIGHTS

All individuals have the following privacy rights under HIPAA:

1. Right to receive a copy of the Notice of Privacy Practices.
2. Right to inspect and copy their PHI.
3. Right to request an amendment of their PHI.
4. Right to request a restriction on the uses and disclosures of PHI.
5. Right to request confidential communication.
6. Right to an accounting of disclosure of PHI.
7. Right to file a complaint.

Patients may ask  
you about their  
privacy rights so  
pay close  
attention!

**ICBHS may not require an  
individual to waive his or her  
rights under HIPAA.  
See ICBHS Policy 01-76.**

HIPAA - The Privacy Rule

42

# INDIVIDUAL PRIVACY RIGHTS

## 1. Privacy Practices Notice

- ▶ All individuals have the right to receive a Notice of Privacy Practices (NOPP)
  - ▶ The NOPP summarizes how ICBHS uses and discloses PHI.
  - ▶ It describes the individual's rights with respect to PHI
  - ▶ It describes the legal obligations of ICBHS to protect privacy, provide a notice of privacy practices, and abide by the terms of the current privacy notice
  - ▶ It provides information on how to file a complaint with the ICBHS Privacy Officer or the Secretary of the US Department of Health and Human Services

43

HIPAA - The Privacy Rule

43

# INDIVIDUAL PRIVACY RIGHTS

## 1. Privacy Practices Notice

- ▶ Staff must try to obtain acknowledgment from the individual that he/she received the NOPP:
  - ▶ Provided on first visit during the UMDAP process prior to treatment (in an emergency the NOPP may be provided as soon as practicable after the emergency subsides)
  - ▶ Staff documents that the NOPP was given by having the individual sign and date the Notice of Privacy Practices Acknowledgment Form
  - ▶ Provide a copy of the acknowledgment form to the individual
- ▶ Staff should document the attempt if the individual doesn't complete the acknowledgment
- ▶ Scan a copy of the acknowledgment into the individual's electronic health record

44

HIPAA - The Privacy Rule

44

# INDIVIDUAL PRIVACY RIGHTS

## 1. Privacy Practices Notice

- ▶ The NOPP is available at all sites accessible by ICBHS patients and visitors. Posters are also posted at all sites to inform ICBHS patients of their privacy rights.
- ▶ The Compliance Unit conducts periodic site visits to ensure the NOPP brochure and poster are clearly visible at all sites accessible by ICBHS patients.
- ▶ The NOPP is also required to be posted on the ICBHS website. You can find it under the Resources section of <https://bhs.imperialcounty.org>.
- ▶ **ICBHS Policy 01-63** provides more information about the NOPP.

45

HIPAA - The Privacy Rule

45

# INDIVIDUAL PRIVACY RIGHTS

## 2. Right to Inspect and Copy

- ▶ Individuals have the right to review and obtain a copy of their PHI. See **ICBHS Policy 01-65**. Requests must be submitted in writing.
- ▶ Requests to access, inspect, and copy PHI should be evaluated by a *professional who has the authority to determine if the request should be granted or denied*.
- ▶ **ICBHS Procedure 01-29** outlines the steps that should be followed when granting an individual access to inspect and obtain a copy of his or her PHI.

46

HIPAA - The Privacy Rule

46

# INDIVIDUAL PRIVACY RIGHTS

## 2. Right to Inspect and Copy

- ▶ If the request is denied, the individual must be provided with a written denial. See **ICBHS Policy 01-66** and **ICBHS Procedure 01-30**.
- ▶ Examples of situations where access may be denied or delayed:
  - ▶ Psychotherapy notes
  - ▶ PHI that is compiled for legal proceedings
  - ▶ Access would endanger a person's life or safety based upon a professional judgment
    - ▶ In this situation, the individual must be given the right to have such denials reviewed by a licensed health care professional for a second opinion. See **ICBHS Procedure 01-31**.

47

HIPAA - The Privacy Rule

47

# INDIVIDUAL PRIVACY RIGHTS

## 2. Right to Inspect and Copy

- ▶ Under California law, ICBHS must provide access to inspect during business hours within 5 working days of receiving the written request.
- ▶ ICBHS may provide a summary of the PHI requested, under certain circumstances. The summary must be provided within 10 working days of receiving the written request.
- ▶ Copies of the PHI must be transmitted within 15 calendar days of receiving the written request.

48

HIPAA - The Privacy Rule

48



# INDIVIDUAL PRIVACY RIGHTS

## 2. Right to Inspect and Copy

- ▶ When a covered entity uses an electronic health record (we do!), the individual has the right to request an electronic copy of his or her record.
- ▶ The individual can direct a covered entity to transmit information to a third party specified by an individual.

49

HIPAA - The Privacy Rule

49

# INDIVIDUAL PRIVACY RIGHTS

## 3. Right to Request an Amendment or Addendum

- ▶ Individuals may request either an amendment or an addendum to their medical record if they feel that information is inaccurate or incomplete. See **ICBHS Policy 01-67**. Requests must be submitted in writing.
- ▶ The request for an amendment must be acted upon within 60 calendar days of receiving the written request.
- ▶ **ICBHS Procedure 01-13** outlines the steps to be followed when granting a request to amend PHI.

50

HIPAA - The Privacy Rule

50

# INDIVIDUAL PRIVACY RIGHTS

## 3. Right to Request an Amendment or Addendum

- ▶ A request may be denied if:
  - ▶ The information is accurate and complete according to the health care professional that wrote it; or,
  - ▶ It was not created by ICBHS.
- ▶ If the request is denied, the individual must be provided with a written denial. See **ICBHS Policy 01-91**, **ICBHS Procedure 01-14**, and **ICBHS Procedure 01-28** for more information.

51

HIPAA - The Privacy Rule

51

# INDIVIDUAL PRIVACY RIGHTS

## 4. Right to Request a Restriction

- ▶ Individuals have the right to request restrictions on the use and disclosure of their PHI as it relates to:
  - ▶ Treatment, payment, or health care operations; or,
  - ▶ Notifying family members or others about the individual's general condition, location, or death (as permitted under Permitted Uses and Disclosures – Opportunity to Agree or Object). See 45 CFR § 164.510(b).
- ▶ Requests for restriction should be submitted in writing. Requests are reviewed, approved, and communicated by the ICBHS Privacy Officer. See **ICBHS Policy 01-69** and **Procedure 01-21** for more information.
- ▶ Requests submitted to staff should be forwarded to the ICBHS Privacy Officer within one working day of receipt.

52

HIPAA - The Privacy Rule

52

# INDIVIDUAL PRIVACY RIGHTS

## 5. Right to Request Confidential Communications

- ▶ Individuals have the right to request an alternative means or location for receiving communications of PHI by means other than those that the covered entity typically utilizes.
- ▶ Requests for confidential communications should be submitted in writing. Requests are reviewed, approved, and communicated by the ICBHS Privacy Officer. See **ICBHS Policy 01-73** and **Procedure 01-19** for more information.
- ▶ Requests submitted to staff should be forwarded to the ICBHS Privacy Officer within one working day of receipt.

53

HIPAA - The Privacy Rule

53

# INDIVIDUAL PRIVACY RIGHTS

## 6. Right to an Accounting of Disclosures

- ▶ Individuals have the right to an accounting of the disclosures of their PHI by a covered entity or the covered entity's business associates. The maximum disclosure accounting period is 6 years prior to the date of the request.
- ▶ The response to the request must be made in writing and include the following for each disclosure:
  - ▶ Date of disclosure;
  - ▶ Name and address of the person or entity who received the PHI;
  - ▶ A brief description of the PHI disclosed; and,
  - ▶ A brief statement of the purpose of the disclosure.

54

HIPAA - The Privacy Rule

54

## INDIVIDUAL PRIVACY RIGHTS

### 6. Right to an Accounting of Disclosures

- ▶ The request for an accounting of disclosures must be acted upon no later than 60 calendar days following receipt of the request.
- ▶ **ICBHS Policy 01-68** and **Procedure 01-15** provide detailed information on how to process requests for an accounting of disclosures.

55

HIPAA - The Privacy Rule

55

## INDIVIDUAL PRIVACY RIGHTS

### 6. Right to an Accounting of Disclosures

- ▶ Disclosures **NOT** required to be included on the accounting of disclosures include the following:
  1. For treatment, payment, or operations;
  2. To the individual or the individual's representative;
  3. For notification of or to persons involved in an individual's health care or payment for health care, for disaster relief, or for facility directories;
  4. Pursuant to the individual's signed authorization;
  5. As part of a limited data set;
  6. For national security or intelligence purposes;
  7. To correctional institutions or law enforcement officials for certain purposes regarding inmates or individuals in lawful custody; and,
  8. Incident to an otherwise permitted or required disclosure.

56

HIPAA - The Privacy Rule

56

## INDIVIDUAL PRIVACY RIGHTS

### 6. Right to an Accounting of Disclosures

- Disclosures **REQUIRED** to be included on the accounting of disclosures include the following:
  - ▶ Those required by law
  - ▶ Releases made in error (i.e. breaches)
  - ▶ To avert threat to health and safety
  - ▶ For law enforcement purposes
  - ▶ For judicial/administrative proceedings
  - ▶ For victims of abuse, neglect, or violence
  - ▶ For public health activities
  - ▶ For Health oversight activities
  - ▶ For Organ/eye/tissue donations
  - ▶ For research purposes
  - ▶ For specialized government functions
  - ▶ About decedents
  - ▶ For Workers' Compensation

57

HIPAA - The Privacy Rule

57

## INDIVIDUAL PRIVACY RIGHTS

### 7. Right to File a Complaint

- ▶ Individuals have the right to complain if they think that their privacy rights have been violated. Complaints may be submitted orally or in writing. See **ICBHS Policy 01-70**.
- ▶ The ICBHS Privacy Officer will investigate all privacy complaints according to **ICBHS Procedure 01-20**. Individuals may contact the ICBHS Privacy Officer directly regarding their complaint. If ICBHS staff or contractors receive a privacy complaint, it should be immediately forwarded to the ICBHS Privacy Officer. This includes privacy complaints submitted through the Medi-Cal beneficiary grievance process.

58

HIPAA - The Privacy Rule

58

## POLL #5

59

59

## ADMINISTRATIVE REQUIREMENTS

HIPAA imposes the following administrative requirements on covered entities:

- ▶ Establishment of privacy policies and procedures
- ▶ Designation of a Privacy Officer
- ▶ Establishment of a complaint process
- ▶ Implementation of a non-retaliation policy
- ▶ Workforce training
- ▶ Mitigation of harmful effects of improper use and disclosure of PHI
- ▶ Documentation and record retention
- ▶ Safeguards for written, spoken, and electronic PHI

60

HIPAA - The Privacy Rule

60

# ADMINISTRATIVE REQUIREMENTS

## Privacy Policies and Procedures

- ▶ Covered entities must develop and implement written privacy policies and procedures that are consistent with the Privacy Rule. See **ICBHS Policy 01-62**.
- ▶ The privacy policies and procedures implemented by ICBHS are referenced throughout this training. You may request copies of these documents from your immediate supervisor or obtain them from the ICBHS Intranet.

61

HIPAA - The Privacy Rule

61

# ADMINISTRATIVE REQUIREMENTS

## Designation of a Privacy Officer

- ▶ Covered entities must designate a Privacy Officer responsible for developing and implementing its privacy policies and procedures. See **ICBHS Policy 01-77**.
- ▶ The ICBHS Privacy Officer oversees ICBHS compliance with the Privacy Rule and also investigates privacy complaints.
- ▶ The current ICBHS Privacy Officer is Sarah Moore, Behavioral Health Manager.

62

HIPAA - The Privacy Rule

62

# ADMINISTRATIVE REQUIREMENTS

## Establishment of a Complaint Process

- ▶ A covered entity must have procedures for individuals to complain about its compliance with its privacy policies and procedures and the Privacy Rule. These procedures must also be explained in the Notice of Privacy Practices.
- ▶ Any individual or workforce member may make a privacy complaint with the ICBHS Privacy Officer, as indicated in **ICBHS Policy 01-70**. The ICBHS Privacy Officer will investigate all privacy complaints according to **ICBHS Procedure 01-20**.

63

HIPAA - The Privacy Rule

63

## How to Contact the ICBHS Privacy Officer

### **In Person**

Sarah Moore  
202 N. 8<sup>th</sup> Street  
El Centro, CA 92243

### **Call or Email Directly**

442-265-1560

[ICBHSPrivacyOfficer@co.imperial.ca.us](mailto:ICBHSPrivacyOfficer@co.imperial.ca.us)

### **Make a Written Complaint**

Imperial County Behavioral Health Services  
Attn: Compliance Unit  
PO Box 1766  
El Centro, CA 92244

### **Make an Anonymous Complaint via Telephone**

Call the Compliance Hotline at 1-866-314-7240

64

HIPAA - The Privacy Rule

64



# ADMINISTRATIVE REQUIREMENTS

## Non-Retaliation Policy

- ▶ A covered entity may not retaliate in any form against a person for:
  - ▶ Exercising rights provided by the Privacy Rule, including making a privacy complaint
  - ▶ Assisting in an investigation by HHS or another appropriate authority
  - ▶ Opposing an act or practice that the person believes in good faith violates the Privacy Rule.
- ▶ See **ICBHS Policy 01-61**. Any concerns regarding possible relation may be addressed with the ICBHS Privacy Officer.

65

HIPAA - The Privacy Rule

65

# ADMINISTRATIVE REQUIREMENTS

## Workforce Training

- ▶ A covered entity must train all workforce members on its privacy policies and procedures, as necessary and appropriate for them to carry out their functions. See **ICBHS Policy 01-86**.
- ▶ Training must occur **prior** to accessing PHI and no later than 30 days from the date of hire. Ongoing training must be completed at least annually.

66

HIPAA - The Privacy Rule

66

# ADMINISTRATIVE REQUIREMENTS

## Mitigation

- ▶ A covered entity must mitigate, to the extent practicable, any harmful effect it learns was caused by use or disclosure of protected health information by its workforce or its business associates in violation of its privacy policies and procedures or the Privacy Rule.
- ▶ **ICBHS Policy 01-87** establishes possible mitigation actions, including, but not limited to:
  - ▶ Retrieval of the information, where possible.
  - ▶ An apology letter to the client.
  - ▶ Addressing and investigating employee violations
  - ▶ Taking employment action to retrain, reprimand, or discipline employees as necessary

67

HIPAA - The Privacy Rule

67

# ADMINISTRATIVE REQUIREMENTS

## Mitigation

- ▶ **ICBHS Policy 01-60** establishes the following severity levels for privacy violations:
  - ▶ Level 1: Accidental and/or unintentional disclosure of PHI or records
  - ▶ Level 2: Deliberate violation
  - ▶ Level 3: Willful neglect and malicious violation
- ▶ The ICBHS Privacy Officer will investigate all potential privacy violations before disciplinary action is taken.

68

HIPAA - The Privacy Rule

68

# ADMINISTRATIVE REQUIREMENTS

## Mitigation

- ▶ Recommended disciplinary actions include:
  - ▶ **For Level 1**, accidental and/or unintentional disclosure of PHI or records:
    - ▶ Verbal caution
    - ▶ Retraining on privacy and security awareness
    - ▶ Retraining on ICBHS privacy and security policies
    - ▶ Retraining on internal controls and forms
  - ▶ **For Level 2**, deliberate violation:
    - ▶ Consider disciplinary action taken for Level 1 which may be combined with additional actions below if appropriate
    - ▶ Written reprimand or suspension
    - ▶ Retraining on potential civil and criminal prosecution associated with privacy and security violations

69

HIPAA - The Privacy Rule

69

# ADMINISTRATIVE REQUIREMENTS

## Mitigation

- ▶ Recommended disciplinary actions include:
  - ▶ **For Level 3**, willful neglect and malicious violation:
    - ▶ Consider disciplinary action taken for Level 1 and/or Level 2 which may be combined with additional actions below if appropriate
    - ▶ Disciplinary action up to and including termination
    - ▶ Retraining on potential civil and criminal prosecution associated with privacy and security violations
  - ▶ Additionally, workforce members who knowingly and willfully violate state or federal law for failure to safeguard PHI are subject to criminal investigation, prosecution, and/or civil monetary penalties.

70

HIPAA - The Privacy Rule

70

# ADMINISTRATIVE REQUIREMENTS

## Documentation and Record Retention

- ▶ A covered entity must maintain, until six years after the later of the date of their creation or last effective date, its privacy policies and procedures, its privacy practices notices, disposition of complaints, and other actions, activities, and designations that the Privacy Rule requires to be documented. See **ICBHS Policy 01-75**.

71

HIPAA - The Privacy Rule

71

# ADMINISTRATIVE REQUIREMENTS

## Data Safeguards

- ▶ A covered entity must maintain reasonable and appropriate administrative, technical, and physical safeguards to prevent intentional or unintentional use or disclosure of PHI in violation of the Privacy Rule and to limit its incidental use and disclosure pursuant to otherwise permitted or required use or disclosure.
- ▶ All ICBHS staff, providers, and contractors must ensure that PHI is safeguarded from unauthorized uses and disclosures, loss, or destruction. ***This applies to all written, oral, and electronic PHI.***

72

HIPAA - The Privacy Rule

72

# ADMINISTRATIVE REQUIREMENTS

## Data Safeguards

Where is written PHI?

- ▶ In file cabinets
- ▶ On or in our desks
- ▶ Near fax machines, printers, and copiers
- ▶ On white board
- ▶ In staff mailboxes



73

HIPAA - The Privacy Rule

73

# ADMINISTRATIVE REQUIREMENTS

## Data Safeguards

Where is oral PHI?

- ▶ In conversations we have about clients
- ▶ When we talk on the phone
- ▶ Phone messages left on voicemail



74

HIPAA - The Privacy Rule

74

# ADMINISTRATIVE REQUIREMENTS

## Data Safeguards

Where is electronic PHI?

- ▶ Saved on our computers
- ▶ Included in our emails



75

HIPAA - The Privacy Rule

75

# ADMINISTRATIVE REQUIREMENTS

## Data Safeguards

Some ways to protect PHI:

- ▶ Don't leave PHI unattended on your desk or workstation – this means not leaving PHI underneath your calendars, mixed in with other papers, or in storage shelves/bins
- ▶ Don't leave your EHR open when you are not using it
- ▶ Don't leave your computer unattended without logging out
- ▶ Lock your file cabinets when not in use – especially when you leave for the day
- ▶ Remove PHI from copy machines, printers, and fax machines right away
- ▶ Lock PHI in the trunk of the vehicle when traveling

76

HIPAA - The Privacy Rule

76

# ADMINISTRATIVE REQUIREMENTS

## Data Safeguards

Some ways to protect PHI:

- ▶ Do not talk about clients in public places
- ▶ Do not talk about clients to anyone not involved in the client's care
- ▶ Lower the volume when playing voicemails
- ▶ Avoid discussing PHI in public areas
- ▶ When conducting telehealth appointments, ensure you are in a private space and not in a shared area
- ▶ Encrypt emails that include PHI

77

HIPAA - The Privacy Rule

77

Most importantly...

**Protect a client's information as if it was your own.**

78

HIPAA - The Privacy Rule

78

**POLL #6**

79

79

**BREAK**

80

80



## THE SECURITY RULE



81

81

## THE SECURITY RULE - INTRODUCTION

The Security Rule establishes a national set of security standards for protecting certain health information that is held or transferred in electronic form. The Security Rule operationalizes the protections contained in the Privacy Rule by addressing the technical and non-technical safeguards that covered entities must put in place to secure individuals' "electronic protected health information" (ePHI).

A major goal of the Security Rule is to protect the privacy of individuals' PHI while allowing covered entities to adopt new technologies to improve the quality and efficiency of patient care.

82

82

## WHO IS COVERED BY THE SECURITY RULE?

- ▶ Like the Privacy Rule, the following are covered by the Security Rule:
  - ▶ Health Plans
  - ▶ Health Care Providers
  - ▶ Clearinghouses
  - ▶ Business Associates

83

HIPAA - The Security Rule

83

## WHAT INFORMATION IS PROTECTED BY THE SECURITY RULE?

- ▶ The Security Rule protects electronic protected health information (ePHI)
- ▶ ePHI = all individually identifiable information that a covered entity creates, receives, maintains, or transmits in electronic form
- ▶ Remember, individually identifiable health information is information that relates to:
  - ▶ The individual's past, present or future physical or mental health condition,
  - ▶ The provision of health care to the individual, or
  - ▶ The past, present, or future payment for the provision of health care to the individual,
  - ▶ AND that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual.

84

HIPAA - The Security Rule

84

## WHAT INFORMATION IS PROTECTED BY THE SECURITY RULE?

Components of identifiable information include:

- ▶ Name
- ▶ Address
- ▶ Certificate/License Number
- ▶ Elements of dates related to a patient, such as date of birth, admission date, or discharge date
- ▶ Telephone and/or fax number
- ▶ Social Security number
- ▶ Email Address
- ▶ Medical Record Number
- ▶ Health Plan Beneficiary Number
- ▶ Account Number (BC#)
- ▶ Any vehicle or device serial number, including license plate
- ▶ Web addresses (URLs)
- ▶ Internet Protocols (IP) Address
- ▶ Finger or voice prints
- ▶ Photographic images
- ▶ Age greater than 89 (as the 90 year old population is very small)
- ▶ Any other unique identifying number/characteristic/code

85

HIPAA - The Security Rule

85

## GENERAL RULES

The Security Rule requires covered entities to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting ePHI. Specifically, covered entities must:

1. Ensure the confidentiality, integrity, and availability of all ePHI they create, receive, maintain or transmit;
2. Identify and protect against reasonably anticipated threats to the security or integrity of the information;
3. Protect against reasonably anticipated, impermissible uses or disclosures; and
4. Ensure compliance by their workforce.

86

HIPAA - The Security Rule

86

## GENERAL RULES

The Security Rule defines "confidentiality" to mean that ePHI is not available or disclosed to unauthorized persons. The Security Rule's confidentiality requirements support the Privacy Rule's prohibitions against improper uses and disclosures of PHI.

The Security Rule also promotes the two additional goals of maintaining the integrity and availability of ePHI. Under the Security Rule, "integrity" means that ePHI is not altered or destroyed in an unauthorized manner. "Availability" means that ePHI is accessible and usable on demand by an authorized person.

87

HIPAA - The Security Rule

87

## GENERAL RULES

1

### Confidentiality

PHI is not accessible to unauthorized individuals

2

### Availability

PHI is accessible on-demand when necessary and appropriate

3

### Integrity










PHI is not improperly altered or destroyed

88

HIPAA - The Security Rule

88

## GENERAL RULES

Examples	Confidentiality	Integrity	Availability
Electronic Health Record (Server)			
Locked File Cabinet			
Unlocked File Cabinet			

89

HIPAA - The Security Rule

89

## RISK ANALYSIS AND MANAGEMENT

The Security Rule requires covered entities to perform risk analysis as part of their security management processes. A risk analysis process may include:

- ▶ Evaluating the likelihood and impact of potential risks to ePHI
- ▶ Implementing appropriate security measures to address the risks identified in the risk analysis
- ▶ Documenting the chosen security measures and, where required, the rationale for adopting those measures
- ▶ Maintaining continuous, reasonable, and appropriate security protections

90

HIPAA - The Security Rule

90

## RISK ANALYSIS AND MANAGEMENT

ICBHS' risk analysis and management process is two-fold:

1. Conducting ongoing monitoring activities, such as reviewing and verifying access to the Electronic Health Record and conducting on-site security inspections
2. Contracting with an agency to conduct a security risk assessment, which involves (1) an analysis of the privacy and security threats to paper and electronic PHI that is stored, created, transmitted, and maintained by ICBHS and (2) an evaluation of the safeguards ICBHS has in place

The Information Systems and Compliance Units work together to mitigate potential risks. See **ICBHS Policies 01-289** and **01-296** for more information.

91

HIPAA - The Security Rule

91

## SAFEGUARDS

The Security Rule requires covered entities to have the following safeguards in place:

- ▶ Administrative Safeguards – administrative actions, policies, and procedures to manage the selection, development, implementation, and maintenance of security measures to protect ePHI and to manage the workforce in relation to the protection of that information
- ▶ Physical Safeguards – technology and the policies and procedures for its use that protect ePHI and controls access to it.
- ▶ Technical Safeguards – physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

92

HIPAA - The Security Rule

92

# ADMINISTRATIVE SAFEGUARDS

## Security Management Process

- ▶ A covered entity must identify and analyze potential risks to ePHI and must implement security measures that reduce risks and vulnerabilities to a reasonable and appropriate level.
- ▶ In addition to the security risk analysis and management process mentioned previously, ICBHS has several policies and procedures that outline how safeguards are to be carried out and by whom.

93

HIPAA - The Security Rule

93

# ADMINISTRATIVE SAFEGUARDS

## Security Management Process – ICBHS Policies and Procedures:

- **Policy 01-22**, HIPAA-Authorization for the Use and Disclosure of Protected Health Information
- **Policy 01-69**, HIPAA-Request for Special Restriction on the Uses and Disclosures of Protected Health Information
- **Policy 01-77**, HIPAA-Privacy and Security Roles
- **Policy 01-86**, HIPAA-Security and Privacy Training
- **Policy 01-88**, HIPAA-Business Associates
- **Policy 01-100**, HIPAA-Password and User ID Controls
- **Policy 01-158**, HIPAA-Security Incident Notification and Mandatory Reporting
- **Policy 01-191**, HIPAA-Breach Notification and Mandatory Reporting
- **Policy 01-231**, HIPAA-User Access Management
- **Policy 01-232**, HIPAA-PHI Protection
- **Policy 01-234**, HIPAA-Workstation Security

94

HIPAA - The Security Rule

94

# ADMINISTRATIVE SAFEGUARDS

## Security Management Process – ICBHS Policies and Procedures:

- **Policy 01-235**, HIPAA-Mobile Device and Media Security
- **Policy 01-237**, HIPAA-Security Incident Reporting and Response
- **Policy 01-247**, HIPAA-Malicious Spyware
- **Policy 01-289**, HIPAA-Risk Management
- **Policy 01-290**, HIPAA-Security Management
- **Policy 01-291**, HIPAA-Physical Security
- **Policy 01-295**, HIPAA-Perimeter, Remote Access, and Wireless Security
- **Policy 01-296**, HIPAA-Information System Monitoring
- **Policy 01-297**, HIPAA-Contingency Plan
- **Procedure 01-163**, HIPAA-PHI Inventory
- **Procedure 01-164**, HIPAA-Encryption
- **Procedure 01-166**, HIPAA-Access Control
- **Procedure 01-167**, HIPAA-Workstation Configuration
- **Procedure 01-168**, HIPAA-Reporting a Potential Privacy Breach to the HIPAA Privacy Officer or Designee

95

HIPAA - The Security Rule

95

# ADMINISTRATIVE SAFEGUARDS

## Security Personnel

- ▶ A covered entity must designate a security official who is responsible for developing and implementing its security policies and procedures.
- ▶ The current ICBHS Security Officer is Sarah Moore, Behavioral Health Manager. Any security incidents may be reported to her directly by phone at 442-265-1560 or via email at [ICBHSPrivacyOfficer@co.imperial.ca.us](mailto:ICBHSPrivacyOfficer@co.imperial.ca.us).
- ▶ Report security incidents immediately. See **ICBHS Policies 01-158** and **01-237**.
- ▶ The longer an incident goes unreported, the more damage it can cause.

96

HIPAA - The Security Rule

96



# ADMINISTRATIVE SAFEGUARDS

## Information Access Management

- ▶ The Security Rule requires a covered entity to implement policies and procedures for authorizing access to ePHI only when such access is appropriate based on the user or recipient's role (role-based access). **ICBHS Policy 01-231** establishes the rules for authorizing access to ePHI.
- ▶ **Management and supervisory staff** play a large role in enforcing information access management by providing timely notification to the Information Systems Unit whenever staff user roles change as a result of new assignments, promotion, or separation from ICBHS.

97

HIPAA - The Security Rule

97

# ADMINISTRATIVE SAFEGUARDS

## Workforce Training and Management

- ▶ A covered entity must provide for appropriate authorization and supervision of workforce members who work with ePHI. Authorization is granted through the Information Systems and monitored for appropriateness on a regular basis.
- ▶ All workforce members must also be trained regarding security policies and procedures.
- ▶ A covered entity must also have and apply appropriate sanctions against workforce members who violate its policies and procedures. See **ICBHS Policy 01-60** and **ICBHS Procedure 01-33**.

98

HIPAA - The Security Rule

98

# ADMINISTRATIVE SAFEGUARDS

## Evaluation

- ▶ A covered entity must perform a periodic assessment of how well its security policies and procedures meet the requirements of the Security Rule.
- ▶ ICBHS completes this at least annually and updates policies and procedures as needed.

99

HIPAA - The Security Rule

99

# PHYSICAL SAFEGUARDS

## Facility Access and Control

- ▶ A covered entity must limit physical access to its facilities while ensuring that authorized access is allowed. ICBHS implements this according to **ICBHS Policies 01-232** and **01-291**.
- ▶ Examples of facility access controls include:
  - ▶ Keypad doors
  - ▶ Controlled access hours
  - ▶ Security guards
  - ▶ Cameras
  - ▶ ID Badges

100

HIPAA - The Security Rule

100

# PHYSICAL SAFEGUARDS

## Workstation and Device Security

- ▶ A covered entity must implement policies and procedures to specify proper use of and access to workstations and electronic media. A covered entity also must have in place policies and procedures regarding the transfer, removal, disposal, and re-use of electronic media, to ensure appropriate protection of ePHI. ICBHS implements this according to **ICBHS Policies 01-100, 01-234, and 01-235**.
- ▶ Examples:
  - ▶ Locking your computer when you leave your desk.
  - ▶ Locking your workstation when you take a break, leave for lunch, or end your shift.

101

HIPAA - The Security Rule

101

# TECHNICAL SAFEGUARDS

## Access Control

- ▶ A covered entity must implement technical policies and procedures that allow only authorized persons to access ePHI. See **ICBHS Policy 01-231** and **Procedure 01-166**.
- ▶ Access controls are implemented according to the minimum necessary standard.

102

HIPAA - The Security Rule

102

# TECHNICAL SAFEGUARDS

## RECEPTION & FRONT DESK

- Reception View
- Staff Daily Appointments
- Client Reminder



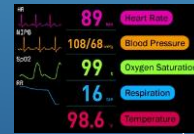
## LPHA/CLINICIAN

- CalAIM Assessment
- CANS
- Service Note



## PRESCRIBER

- Lab Result and Review
- Medication Management (Rx)
- Vitals Signs Report



103

HIPAA - The Security Rule

103

# TECHNICAL SAFEGUARDS

## Audit Control

- ▶ A covered entity must implement hardware, software, and/or procedural mechanisms to record and examine access and other activity in information systems that contain or use ePHI.
- ▶ The Information Systems Unit inventories all tangible and electronic PHI according to **ICBHS Procedure 01-163** and implements a variety of auditing mechanisms to track and verify access to ePHI.

104

HIPAA - The Security Rule

104

# TECHNICAL SAFEGUARDS

## Integrity Controls

- ▶ A covered entity must implement policies and procedures to ensure that ePHI is not improperly altered or destroyed. Electronic measures must be put in place to confirm that ePHI has not been improperly altered or destroyed.
- ▶ An example of this is finalizing a progress note to ensure that the note is not altered or destroyed. Any changes to finalized progress notes if strictly controlled through the Edit Service Request process completed by supervisors and managers.

105

HIPAA - The Security Rule

105

# TECHNICAL SAFEGUARDS

## Transmission Security

- ▶ A covered entity must implement technical security measures that guard against unauthorized access to ePHI that is being transmitted over an electronic network.
- ▶ ICBHS protects against unauthorized access to ePHI according to **ICBHS Policies 01-235, 01-247, and 01-295.**
- ▶ Examples of transmission security include encryption and firewalls.

106

HIPAA - The Security Rule

106

# POLL #7

107

107

# POLL #8

108

108

## ICBHS SECURITY SAFEGUARDS

- ▶ All computers are password protected with individual user access
- ▶ Network Password Criteria:
  - ▶ Must be 12 characters long
  - ▶ Must include 1 upper case letter
  - ▶ Must include 1 lower case letter
  - ▶ Must include 1 special character
  - ▶ Must not include consecutive numbers or letters
  - ▶ Must not include self identifying information
- ▶ Computers are encrypted
- ▶ Most sites utilize the main ITS network, which is the most reliable and secure
  - ▶ School sites and devices used in the field connect utilizing a Virtual Private Network (VPN) which creates a secure connection

HIPAA - The Security Rule

109

## ICBHS SECURITY SAFEGUARDS

- ▶ Individual Electronic Health Care access
- ▶ Passwords:
  - ▶ Must be at least 14 characters
  - ▶ Must include 1 lower case letter(a-z)
  - ▶ Must include 1 Upper case letter (A-Z)
  - ▶ Must include 1 Numbers ( 0-9 )
  - ▶ Must include a special character
  - ▶ Password must be changed every 90 days
  - ▶ Can't use passwords that have been used in the past
- ▶ Call 442-265-1586 or submit a ManageEngine ticket to reset your password

Streamline  
Healthcare Solutions, LLC.

Username  
Enter Username

Password  
Enter Password

Remember me

LOGIN

Forgot your Username?      Forgot your Password?

Copyright © 2022 - 2023 Streamline Healthcare Solutions, LLC. All Rights Reserved.

HIPAA - The Security Rule

110

# ICBHS SECURITY SAFEGUARDS

## Security Questions

- 3 questions
- Case Sensitive
- Questions will reset after each password reset

## Two-Factor Authentication (2FA)

- Set for every other day
- Associated with your work email

111

HIPAA - The Security Rule

111

# ICBHS SECURITY SAFEGUARDS

- ▶ All emails containing ePHI **must** be encrypted
  - ▶ If sending an email to someone with [@co.imperial.ca.us](mailto:co.imperial.ca.us) in their email address, the email is encrypted and safe
  - ▶ If sending an email to someone with a different address (i.e. [@dss.ca.gov](mailto:dss.ca.gov) or [@imperial.courts.gov](mailto:imperial.courts.gov)) the email must be manually encrypted

Before you click send, **always:**

- 1) **Make sure the person(s) should be receiving the ePHI you are sending**
- 2) **Verify that your email is encrypted**

112

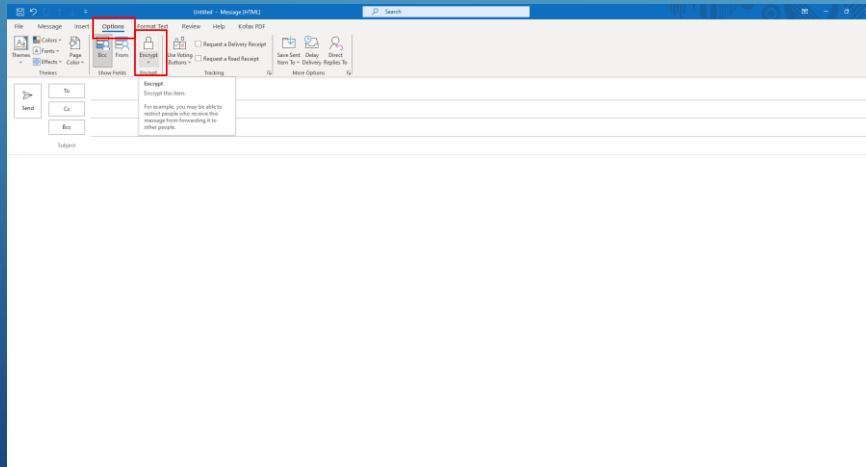
HIPAA - The Security Rule

112



# HOW TO SEND AN ENCRYPTED EMAIL VIA OUTLOOK

1. In the email that you will be drafting, select "Options"
2. Click on the "Encrypt" icon

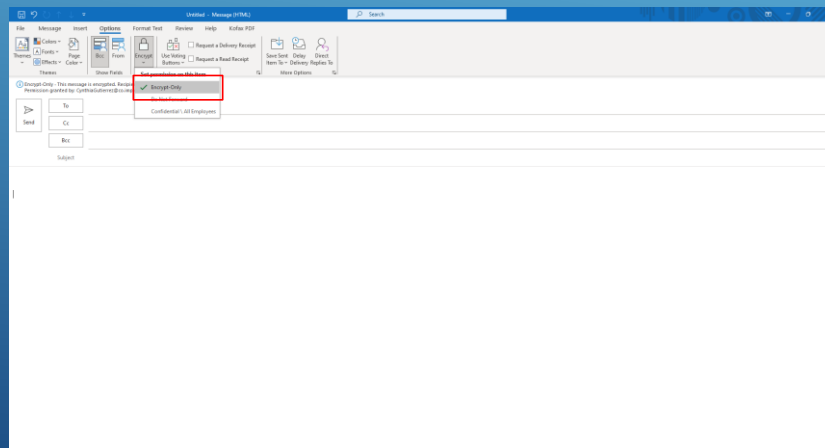


113

113

# HOW TO SEND AN ENCRYPTED EMAIL VIA OUTLOOK

- ▶ 3. Select "Encrypt Only"

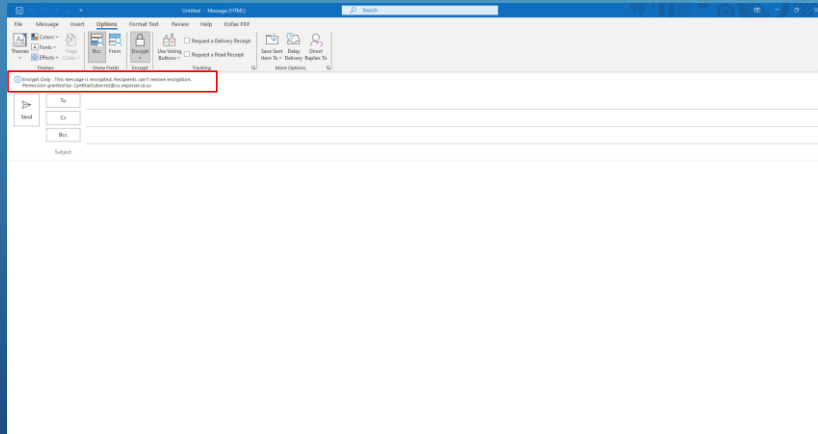


114

114

## HOW TO SEND AN ENCRYPTED EMAIL VIA OUTLOOK

- ▶ 4. Once the email is encrypted, the "Encrypted Only" message will appear on the email you are drafting



115

115

IF YOU HAVE ANY QUESTIONS OR NEED  
ASSISTANCE ON HOW TO ENCRYPT  
EMAILS, CONTACT:

**INFORMATION SYSTEMS**

**442-265-1586**

116

116

## ICBHS SECURITY SAFEGUARDS

### ▶ ICBHS Policy 01-28, Internet and Email

- ▶ Internet services and email are to support the advancement of business goals and objectives
- ▶ Use of computer resources and networks must be business oriented
- ▶ Accessing sites with offensive material is prohibited
- ▶ Emails for the purpose of transmitting obscene, harassing, offensive, or unprofessional messages are prohibited

**The Internet and County email are not private.** All internet and email use is managed and monitored by County of Imperial Information Technology Services.

117

HIPAA - The Security Rule

117

## ICBHS SECURITY SAFEGUARDS

### ▶ County of Imperial Information Technology Services (ITS) Policy:

- ▶ Workforce is expected comply with internet, email, and security policies
- ▶ Assigned IT resources are to exist in the performance of job duties
- ▶ Never download or install any hardware or software without approval from ICBHS or ITS
- ▶ Conducting unauthorized business or commercial activities is prohibited (i.e. buying or selling anything over the Internet)
- ▶ Be aware of malicious software and viruses that attempt to interfere with computer operation, destroy information, or spread through the network
  - ▶ Malicious software and viruses are often transmitted via email, documents attached to email, or Internet

118

HIPAA - The Security Rule

118

## WHAT ROLE DO I PLAY IN SECURING EPHI?

There is a lot of information to digest from this training, so here are some key things you can do to help protect the ePHI you have access to:

- ▶ Lock your computer workstation (CTRL + ALT + DEL or WIN + L)
- ▶ Lock up mobile devices such as laptops, tablets, and phones
- ▶ Lock or log out of SmartCare when you are not using it
- ▶ Do not share any of your passwords!
- ▶ Always ensure the emails you are sending that contain ePHI are encrypted.
- ▶ Do not access ePHI on a mobile device that is not approved by ICBHS Information Systems, this includes accessing your email on your personal phone
- ▶ Learn to recognize phishing scams

119

HIPAA - The Security Rule

119

## PHISHING SCAMS

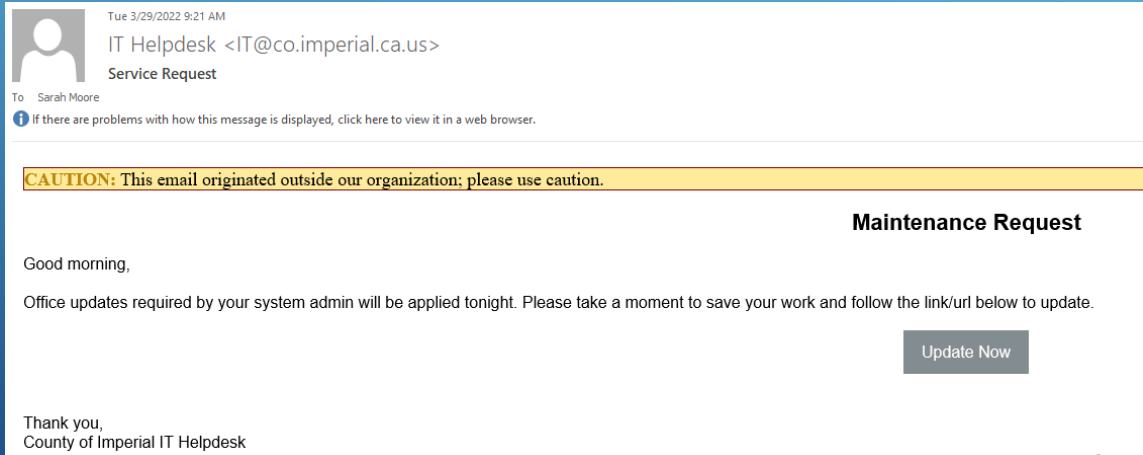
Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack or the revealing of sensitive information.

120

HIPAA - The Security Rule

120

# PHISHING SCAMS



Tue 3/29/2022 9:21 AM  
IT Helpdesk <IT@co.imperial.ca.us>  
Service Request

To: Sarah Moore

If there are problems with how this message is displayed, click here to view it in a web browser.

**CAUTION: This email originated outside our organization; please use caution.**

**Maintenance Request**

Good morning,

Office updates required by your system admin will be applied tonight. Please take a moment to save your work and follow the link/url below to update.

Update Now

Thank you,  
County of Imperial IT Helpdesk

121

HIPAA - The Security Rule

121

# PHISHING SCAMS

Please follow the following guidelines to avoid falling for a phishing scam:

- ▶ Pay attention to this banner in your County email:

**CAUTION: This email originated outside our organization; please use caution.**

- ▶ Do not click on any links or attachments sent by someone whose email address you don't recognize.
- ▶ Delete suspicious emails.
- ▶ Never respond to electronic requests for user ID and/or password.
- ▶ Report suspicious activity to 442-265-1586 or to the Security Officer.

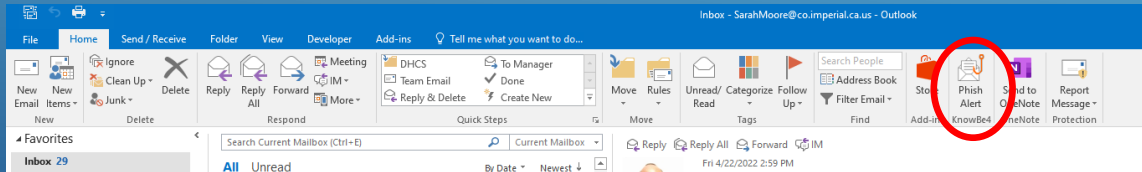
122

HIPAA - The Security Rule

122

# PHISHING SCAMS

You can report potential phishing scams by clicking the Phish Alert button in Microsoft Outlook. If you get a suspicious email, click the Phish Alert button and the email will be deleted from your inbox and forwarded to County ITS for analysis.



123

HIPAA - The Security Rule

123

# PHISHING SCAMS

Key Takeaways:

- ▶ Social engineering is the art of manipulating people, not computers.
- ▶ Scammers craft emails that impersonate real websites or apps.
- ▶ Hasty clicks are dangerous clicks.
- ▶ Slow down and thoroughly inspect emails before taking any action.

124

HIPAA - The Security Rule

124

**The sooner suspicious activity is reported, the sooner it can be investigated and addressed!**

## How to Report Suspicious Activity

### Contact the Security Officer

Sarah Moore  
442-265-1560

[ICBSPrivacyOfficer@co.imperial.ca.us](mailto:ICBSPrivacyOfficer@co.imperial.ca.us)

### Contact Information Systems

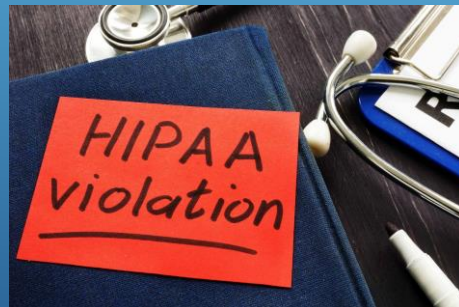
442-265-1586

125

HIPAA - The Privacy Rule

125

## HIPAA ENFORCEMENT



126

126

## WHAT IS A PRIVACY BREACH?

A breach is defined as the acquisition, access, use, or disclosure of unsecured PHI which is not permitted by the Privacy Rule and which compromises the security or privacy of the PHI.

Unsecured PHI is any health information that is not secured through encryption or an approved destruction process that renders the PHI unusable, unreadable, or indecipherable to unauthorized individuals.

127

HIPAA Enforcement

127

## WHAT IS A PRIVACY BREACH?

Examples of potential privacy breaches include:

- ▶ Leaving PHI on a desk, printer, or copy machine over night
- ▶ Sending emails containing ePHI without encryption
- ▶ Sending emails containing ePHI to the wrong person
- ▶ Sending PHI via mail to the wrong recipient
- ▶ Giving out PHI when there is not a proper written authorization on file
- ▶ Discussing a patient's case with family or friends

128

HIPAA Enforcement

128



## PRIVACY & SECURITY INCIDENT SANCTIONS

All members of the ICBHS workforce (employees, volunteers, and trainees) and business associates are required to comply with state and federal laws and regulations, as well as departmental privacy and security policies and procedures.

Any violation of ICBHS privacy and security policies and/or related state and federal laws governing the protection of confidential and client identifiable information may result in disciplinary action depending upon the severity of the act. See **ICBHS Policy 01-60** and **Procedure 01-33**.

129

HIPAA Enforcement

129

## PRIVACY BREACH LEVELS

- ▶ **Level 1** – Improper and/or unintentional disclosure of PHI
  - ▶ Example: Throwing away PHI in a trashcan instead of a shredding box
  
- ▶ **Level 2** – Unauthorized use and/or misuse of PHI
  - ▶ Example: Removing PHI from the workplace
  
- ▶ **Level 3** – Willful and/or intentional disclosure of PHI
  - ▶ Example: Disclosing information in a personal relationship

130

HIPAA Enforcement

130

## PENALTIES FOR BREACHES

In addition to disciplinary action taken by ICBHS (**ICBHS Policy 01-60**), conviction of violating federal and state privacy laws carry the following penalties:

Civil penalties	Up to \$1.5 million per year
Criminal penalties for knowingly obtaining and wrongfully sharing PHI	\$50,000 and 1 year in prison
For obtaining and disclosing PHI through false pretenses	\$100,000 and 5 years in prison
For obtaining and disclosing for commercial advantage, personal gain, or malicious harm	\$250,000 and 10 years in prison

131

HIPAA Enforcement

131

## PENALTIES FOR BREACHES

HHS Office for Civil Rights (OCR) opened an investigation in response to a complaint by a patient alleging that Manasa Health Center posted a response to the patient's negative online review that included specific information regarding the individual's diagnosis and treatment of their mental health condition. In addition to the patient who filed the complaint, OCR's investigation found that Manasa Health Center impermissibly disclosed the protected health information of three other patients in response to their negative online reviews. OCR's investigation also found that Manasa Health Center failed to implement HIPAA Privacy policies and procedures.

Following an OCR investigation, potential violations of the HIPAA Privacy Rule include impermissible disclosures of patient protected health information in response to negative online reviews, and failure to implement policies and procedures with respect to protected health information. Manasa Health Center paid \$30,000 to OCR and agreed to implement a corrective action plan to resolve these potential violations.

132

June 5, 2023 - <https://www.hhs.gov/about/news/2023/06/05/hhs-office-civil-rights-reaches-agreement-health-care-provider-new-jersey-disclosed-phi-response-negative-online-reviews.html>

HIPAA Enforcement

132

## PENALTIES FOR BREACHES

In March 2021, OCR received a complaint alleging that UnitedHealthcare Insurance Company (UHIC) did not respond to an individual's request for a copy of their medical record. The individual first requested a copy of their records on January 7, 2021, but did not receive the records until July 2021, after OCR initiated its investigation. This was the third complaint OCR received from the complainant against UHIC alleging failures to respond to his right of access. OCR's investigation determined that UHIC's failure to provide timely access to the requested medical records was a potential violation of the HIPAA right of access provision. UHIC agreed to implement a corrective action plan and pay \$80,000 to resolve this investigation.

133

HIPAA Enforcement

August 24, 2023 - <https://www.hhs.gov/about/news/2023/08/24/unitedhealthcare-pays-80000-settlement-hhs-resolve-hipaa-matter-patient-medical-records-request.html>

133

## PENALTIES FOR BREACHES

In May 2018, OCR initiated an investigation of Yakima Valley Memorial Hospital following the receipt of a breach notification report, stating that 23 security guards working in the hospital's emergency department used their login credentials to access patient medical records maintained in Yakima Valley Memorial Hospital's electronic medical record system without a job-related purpose. The information accessed included names, dates of birth, medical record numbers, addresses, certain notes related to treatment, and insurance information. To voluntarily resolve this matter, Yakima Valley Memorial Hospital agreed to pay \$240,000 and implement a plan to update its policies and procedures to safeguard protected health information and train its workforce members to prevent this type of snooping behavior in the future. As a result of the settlement agreement, Yakima Valley Memorial Hospital will be monitored for two years by OCR to ensure compliance with the HIPAA Security Rule.

134

HIPAA Enforcement

June 15, 2023 - <https://www.hhs.gov/about/news/2023/06/15/snooping-medical-records-by-hospital-security-guards-leads-240-000-hipaa-settlement.html>

134

## WHO ENFORCES HIPAA?

- ▶ **The Public.** The public is educated about their privacy rights and will not tolerate violations to their privacy.
- ▶ **Office for Civil Rights (OCR).** This is the agency that enforces privacy regulations. They will provide guidance and monitor compliance.
- ▶ **Department of Justice (DOJ).** This agency is involved in criminal privacy violations. They will enact fines, penalties, and imprisonment against offenders.
- ▶ **ICBHS Compliance Unit.** The Compliance Unit conducts routine HIPAA audits and conducts investigations upon receipt of a credible privacy complaint.

135

HIPAA Enforcement

135

## WHAT DO I DO IF THERE IS A PRIVACY BREACH?

Immediately call **Sarah Moore, ICBHS Privacy Officer,**  
at **442-265-1560**

Or call the **Compliance Hotline at 1-866-314-7240**

See **ICBHS Policy 01-191** and **Procedure 01-168.**



REPORTING SYSTEM



136

HIPAA Enforcement

136

## WHAT DO I DO IF THERE IS A SECURITY INCIDENT?



Immediately call **Sarah Moore, ICBHS Security Officer,**  
at **442-265-1560**

Or call the **Information Systems Unit** at **442-265-1586**

See **ICBHS Policies 01-158** and **01-237.**

**The sooner suspicious activity is reported, the sooner  
it can be investigated and addressed!**

HIPAA Enforcement

137

## CALIFORNIA STATE PRIVACY LAWS



138

138

## CALIFORNIA STATE PRIVACY LAWS

- ▶ **Lanterman-Petris-Short Act (LPS)**, Welfare & Institutions Code Section 5328 et seq. – provides special confidentiality protections for medical records containing mental health information.
- ▶ **California Health and Safety Code Section 1280.15** – mandates licensed facilities to report any unlawful or unauthorized access, use, or disclosure of patients' medical information.
- ▶ **California Information Practices Act**, Civil Code Section 1798 – codifies right to privacy as a personal and fundamental right protected by Section 1 of Article 1 of the California Constitution and the United States Constitution
- ▶ **Confidentiality of Medical Information Act**, Civil Code Section 56 et seq. – requires confidentiality of medical information be protected and establishes the protections against disclosures of individually identifiable medical information

139

139

## CALIFORNIA STATE PRIVACY LAWS

- ▶ **Calley's Law (SB 24)**, Family Code Section 6323.5. – authorizes a court to issue an order restraining a party – likely a parent or legal guardian – from accessing records and information pertaining to the health care, education, daycare, recreational activities, or employment of a minor child. As an "essential care provider" ICBHS must comply with a restraining order received under Calley's Law. In the event a parent or legal guardian presents a court order under Calley's Law, ICBHS is prohibited from releasing information or records pertaining to the minor child to the restrained party.
- ▶ The ICBHS Privacy Officer is responsible for receiving the protective order and providing notice to ICBHS staff of the requirement to restrict access to the child's records by the restrained party.

140

140



141

141

## REVIEW

- ▶ HIPAA sets the national standards for the protection of sensitive patient health information.
- ▶ HIPAA applies to ICBHS employees, trainees, volunteers, and contractors.
- ▶ Protected Health Information = PHI
- ▶ PHI can be electronic, paper, or oral and reasonably identifies the patient.
- ▶ Identifiers include (but are not limited to) name, birth date, social security number, BC#, and telephone number.
- ▶ Examples of PHI include patient medical records, mental health or SUD evaluations, and patient demographic information.

142

142

## REVIEW

- ▶ PHI may only be used or disclosed as **permitted or required**.
- ▶ PHI is permitted to be used or disclosed (without an individual's authorization) for the following purposes only:
  - ▶ To the individual;
  - ▶ Treatment, payment, and health care operations;
  - ▶ Opportunity to agree or object;
  - ▶ Incident to an otherwise permitted use and disclosure;
  - ▶ Public interest and benefit activities; and,
  - ▶ Limited data set for the purposes of research, public health, or health care operations.

143

143

## REVIEW

- ▶ A **written** authorization must be obtained for any use or disclosure of PHI that is not permitted or required by HIPAA.
- ▶ **Written** authorization must be obtained prior to use or disclosure of PHI.
- ▶ When in doubt, always make sure you have a written authorization before disclosing PHI.
- ▶ The identity of the recipient of PHI should be verified before the information is disclosed.
- ▶ Only use or disclose the minimum amount of PHI *needed to accomplish the intended purpose of the use, disclosure, or request*. This is known as the Minimum Necessary Standard.

144

144



## REVIEW

- ▶ Patients have individual privacy rights under HIPAA:
  - ▶ Right to receive a copy of the Notice of Privacy Practices.
  - ▶ Right to inspect and copy their PHI.
  - ▶ Right to request an amendment of their PHI.
  - ▶ Right to request a restriction on the uses and disclosures of PHI.
  - ▶ Right to request confidential communication.
  - ▶ Right to an accounting of disclosure of PHI.
  - ▶ Right to file a complaint.

145

145

## REVIEW

- ▶ You can help protect ePHI by ensuring you log out of the EHR when not using it, locking your computer when not using it, verifying who you are sending an email to, and verifying your email is encrypted before sending it.
- ▶ Ensure internet and email use are for business purposes only (i.e. not used for personal reasons).
- ▶ Avoid opening emails from senders you don't recognize.
- ▶ Do not click on any links or attachments sent by someone whose email address you don't recognize.
- ▶ **Never** respond to electronic requests for user ID and/or password.
- ▶ Slow down and thoroughly inspect emails before taking action.
- ▶ Report suspicious activity to 442-265-1856 or to the ICBHS Security Officer, Sarah Moore.

146

146

## REVIEW

- ▶ A privacy breach is the acquisition, access, use, or disclosure of unsecured PHI.
- ▶ Examples of potential privacy breaches include leaving PHI on your desk over night, sending emails containing ePHI without encryption or to the wrong recipient, and disclosing PHI without proper written authorization.
- ▶ Confirmed privacy breaches may result in disciplinary action by ICBHS and/or civil and/or criminal penalties.
- ▶ The ICBHS Privacy Officer is **Sarah Moore**. Potential privacy breaches should be reported to her immediately upon discovery. There is no retaliation for reporting a potential privacy breach.

147

147

## The most important things to remember about HIPAA...

- Only disclose PHI when you have the patient's written authorization, ***unless*** you ***know*** the circumstances allow for an exemption.
- Only disclose the ***minimum necessary*** PHI.
- Treat the patient's health information the same way you would want your private information treated.
- When in doubt, always ask your supervisor before making any type of disclosure.

148

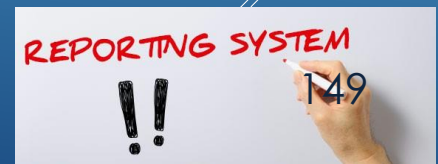
148

## WHAT DO I DO IF THERE IS A PRIVACY BREACH?

Immediately call **Sarah Moore, ICBHS Privacy Officer,**  
at 442-265-1560

Or call the **Compliance Hotline** at 1-866-314-7240

See **ICBHS Policy 01-191** and **Procedure 01-168.**



149

## WHAT DO I DO IF THERE IS A SECURITY INCIDENT?



Immediately call **Sarah Moore, ICBHS Security Officer,**  
at 442-265-1560

Or call the **Information Systems Unit** at 442-265-1586

See **ICBHS Policies 01-158** and **01-237.**

**150**  
The sooner suspicious activity is reported, the sooner  
it can be investigated and addressed!

150

**Thank you for your time!**

**Remember, any questions regarding this training  
or patient privacy-related matters can be  
addressed to:**

**Sarah Moore**, Behavioral Health Manager  
(442) 265-1560

[SarahMoore@co.imperial.ca.us](mailto:SarahMoore@co.imperial.ca.us)

151