COVERED CALIFORNIA

Course Name: Privacy and Security

Participant Guide

Version 1.0

TABLE OF CONTENTS

1. PRIVACY AND SECURITY 1
1.1. LEARNING OBJECTIVES 1
2. LESSON 1: WHAT IS PERSONALLY IDENTIFIABLE INFORMATION (PII)? 1
2.1. LEARNING OBJECTIVES 1
2.1.1. WHAT IS PII? 1
2.1.2. FEDERAL PII 2
2.1.3. INDIVIDUALS' RIGHTS 2
2.1.4 STATE PII 3
2.1.5. SAFEGUARDING PII 4
3. LESSON 2: WHAT IS FEDERAL TAX INFORMATION (FTI)? 4
3.1. LEARNING OBJECTIVES 4
3.1.1. FEDERAL TAX INFORMATION (FTI) 4
3.1.2. WHAT ARE THE SPECIAL PRIVACY AND SECURITY RULES FOR FTI? 4
3.1.3. WHAT ARE THE PENALTIES FOR IMPROPER INSPECTION OR DISCLOSURE OF FTI? 5
3.1.4. REPORTING ANY VIOLATIONS OR SUSPECTED VIOLATIONS OF THE RULES REGARDING FTI 6
3.1.5. LESSON ACTIVITY 1 6
4. LESSON 3: WHAT IS PROTECTED HEALTH INFORMATION (PHI)? 6
4.1. LEARNING OBJECTIVES 6
4.1.1. PROTECTED HEALTH INFORMATION (PHI) 7
4.1.2. INDIVIDUALS' RIGHTS 8
4.1.3. WHAT ARE THE PRIVACY AND SECURITY RULES? 8
4.1.4. WHO MUST FOLLOW THE PRIVACY AND SECURITY RULES? 9
4.1.5. WHEN CAN PHI BE USED AND DISCLOSED? 10
4.1.6. SAFEGUARDS AND THE PRIVACY RULE 11
4.1.7. FILING COMPLAINTS 11
4.1.8. LESSON ACTIVITY 2 12
4.1.9. LESSON ACTIVITY 3 12
5. LESSON 4: INCREASING INFORMATION SECURITY AWARENESS 13
5.1. LEARNING OBJECTIVES 13
5.1.1. INFORMATION SECURITY SAFEGUARDS FOR PROTECTING COVERED CALIFORNIA 13
5.1.2. KEEPING YOUR PASSWORDS SAFE 15
5.1.3. PROTECTING YOUR WORKSTATION, LAPTOP AND MOBILE DEVICE 16
5.1.4. SECURITY WHILE TRAVELING AND WORKING REMOTELY 17
5.1.5. E-MAIL SECURITY 18

5.1.6. PAYMENT CARD SECURITY 19
5.1.7. COMPUTER SECURITY: VIRUSES, MALWARE AND PHISHING 19
5.1.8. SOCIAL MEDIA SAFETY 20
5.1.9. LESSON ACTIVITY 4 21
5.1.10. LESSON ACTIVITY 5 21
5.1.11. LESSON ACTIVITY 6 22
5.1.12. LESSON ACTIVITY 7 22
5.1.13. LESSON ACTIVITY 8 22
6. LESSON 5: PENALTIES FOR VIOLATIONS OF PRIVACY LAWS 22
6.1. LEARNING OBJECTIVES 23
6.1.1. PENALTIES UNDER THE AFFORDABLE CARE ACT, 45, C.F.R. 155.260 23
6.1.2. PENALTIES UNDER THE STATE INFORMATION PRACTICES ACT (IPA) 23
6.1.3. PENALTIES UNDER IRS RULES 23
6.1.4. HIPAA PENALTIES FOR COVERED ENTITIES AND BUSINESS ASSOCIATES 24
6.1.5. CALIFORNIA PENAL CODE PENALTIES 25
6.1.6. EMPLOYEES 25
7. LESSON 6: REPORTING PRIVACY AND SECURITY INCIDENTS 25
7.1. LEARNING OBJECTIVES 25
7.1.1. DUTY TO DETECT AND REPORT INCIDENTS 25
7.1.2. SECURITY INCIDENTS 26
7.1.3. PRIVACY INCIDENTS 26
7.1.4. REPORTING SECURITY AND PRIVACY INCIDENTS 27
7.1.5. IMMEDIATE ACTION IS CRITICAL 27
8. ANSWERS 29
9. ENDNOTES 30

1. Privacy and Security

The Privacy and Security course discusses the definition of personally identifiable information (PII), federal tax information (FTI) and protected health information (PHI), the Health Insurance Portability and Accountability Act (HIPAA) and when this confidential information can be used and disclosed. The course also discusses ways to keep information secure, how to report privacy and security violations and the rights individuals have regarding their personal information.

1.1. Learning Objectives

At the end of this course you will be able to:

- ✓ Define PII, FTI and PHI
- ✓ Know how to protect this confidential information
- ✓ Report privacy and security violations
- ✓ Help individuals with requests regarding their personal information

2. Lesson 1: What Is Personally Identifiable Information (PII)?

In this lesson, you will learn the definition and rules regarding the use of Personally Identifiable Information (PII).

2.1. Learning Objectives

At the end of this lesson you will be able to:

- ✓ Define PII
- ✓ Describe the federal regulations on PII
- ✓ Describe the State Information Practices Act

2.1.1. What is PII?

Personally Identifiable Information ("PII") is any information that identifies or describes an individual. Some examples of information that can be PII include:

- Full Name
- Birthplace
- Email Address
- Vehicle registration plate number
- Credit card numbers
- Country, state, zip code or city of residence
- Name of school attended or workplace
- Social Security Number
- Biometric records
- National Identification number
- Driver's license number
- Age
- Grades, salary or job position
- Date of birth
- Mother's maiden name

2.1.2. FEDERAL PII

The federal regulations under the Affordable Care Act that describe privacy and security requirements for PII in health exchanges such as Covered California can be found in **45 C.F.R. 155.260**. These regulations require Covered California to safeguard the PII it collects, maintains and uses so that no one who is not authorized to access or use the PII can do so. Covered California must also protect the integrity of the PII so that it cannot be altered or destroyed by an unauthorized user. The regulations also limit Covered California to using and disclosing only the PII that is necessary for it to carry out its functions.

The federal regulations governing privacy and security include the following principles:

- ***Individual Access*** - Consumers should be provided with a simple and timely means to access and obtain their PII in a readable form and format
- ***Correction*** - Consumers should be provided with a timely means to dispute the accuracy or integrity of their PII and to have erroneous information corrected or to have a dispute documented if their requests are denied
- ***Openness and transparency*** - There should be openness and transparency about policies, procedures and technologies that directly affect consumers and/or their PII
- ***Individual choice*** - Consumers should be provided a reasonable opportunity and capability to make informed decisions about the collection, use and disclosure of their PII
- ***Collection, use and disclosure limitations*** - PII should be created, collected, used and/or disclosed only to the extent necessary to accomplish a specified purpose(s) and never to discriminate inappropriately
- ***Data quality and integrity*** - Persons and entities should take reasonable steps to ensure that PII is complete, accurate and up-to-date to the extent necessary for the person's or entity's intended purposes and has not been altered or destroyed in an unauthorized manner
- ***Safeguards*** - PII should be protected with reasonable operational, administrative, technical and physical safeguards to ensure its confidentiality, integrity and availability and to prevent unauthorized or inappropriate access, use or disclosure
- ***Accountability*** - These principles should be implemented, and adherence assured, through appropriate monitoring and other means and methods should be in place to report and mitigate non-adherence and breaches.

2.1.3. INDIVIDUALS' RIGHTS

Covered California has implemented the principles of Individual Access, Correction and Individual Choice by adopting procedures to give individuals the following rights:

- Right to request a copy of records with personal information, or to inspect the records
- Right to request correction of records of personal information
- Right to request restrictions on the use and disclosure of personal information
- Right to request confidential communications, so that communications to the individual are sent to the address the individual chooses

- Right to request an accounting of disclosures, showing the date, nature and purpose of disclosures of personal information to other entities
- Right to file a complaint directly with Covered California, alleging Covered California has violated privacy rules

These requests can be made by submitting a written request on the appropriate form. The forms are posted on Covered California's web site. Requests can also be made by the individual's personal representative, by filling out a form for use by such representatives. A complaint form is also posted on the web site.

Covered California has also implemented safeguards to protect the PII it collects and uses in performing its functions. These safeguards are described in a later lesson in this course.

2.1.4 STATE PII

The California law that regulates the collection and use of personal information by state government agencies is the **Information Practices Act of 1977 (IPA)**. The IPA requires all state government agencies to protect the personal information that they maintain and that identifies or describes an individual. Personal information includes:

- Name
- Social security number
- Physical description
- Home address
- Home telephone number
- Education
- Financial matters
- Medical or employment history
- Statements made by or attributed to the individual

The IPA imposes limitations on what a state agency can do with an individual's personal information:

- ***Privacy*** - The IPA states that the right to privacy applies to personal information and that limits must be placed on how the information is obtained and distributed in order to protect the individual.
- ***Collecting Information*** - State agencies are required to collect only information that is relevant to the purpose of the agency and to obtain that information from the individual, rather than a secondhand source, if possible.
- ***Disclosure*** - In order to share the information it has collected, the state agency must have the permission of the individual or demonstrate the legal necessity of disclosing the information.

The IPA also gives rights to individuals pertaining to their personal information, including the following:

- Right to inspect his or her records, which are kept by the state agency and to get a copy of them

- Right to ask the agency to correct or remove information that he or she believes to be erroneous or irrelevant
- Right to see the agency's accounting of disclosures, which shows who has received the individual's records

As set out above in the discussion on the federal regulation, Covered California has implemented procedures so that individuals can exercise these rights. Forms for requesting a copy of records with personal information, corrections to the records, and an accounting of disclosures are posted on the Covered California web site.

2.1.5. SAFEGUARDING PII

Both the federal regulation and the IPA require Covered California to use safeguards to protect PII from any unauthorized users. These safeguards prevent disclosures or uses of the PII that are not permitted and protect the integrity of the PII by preventing any unauthorized users from modifying or destroying the PII. These safeguards will be described in a later lesson in this course.

You must complete privacy and security training before you can access PII and annually thereafter.

3. LESSON 2: WHAT IS FEDERAL TAX INFORMATION (FTI)?

In this lesson, you will learn the definition and rules regarding the use of Federal Tax Information (FTI).

3.1. LEARNING OBJECTIVES

At the end of this lesson you will be able to:

- ✓ Define Federal Tax Information (FTI)
- ✓ Describe the special safeguards needed for FTI
- ✓ Describe the penalties that can result if FTI is improperly used or disclosed

3.1.1. FEDERAL TAX INFORMATION (FTI)

Federal Tax Information (FTI) is information from the Internal Revenue Service (IRS). It is defined as federal tax returns and return information, including any tax information, declaration of estimated tax, claim for refund, a taxpayers' identity, the nature, source or amount of income, payments, receipts, deductions, exemptions, credits, assets, liabilities, net worth, tax liability, tax withheld, deficiencies, over-assessments, or tax payments and other information related to a tax return.

3.1.2. WHAT ARE THE SPECIAL PRIVACY AND SECURITY RULES FOR FTI?

One of the functions that Covered California will perform is reviewing appeals from denials of applications. The Covered California staff responsible for these reviews may access financial records in the process of determining the appeal, and the financial records they access may contain FTI.

The IRS has very strict rules on who is permitted to see FTI. FTI can only be accessed by persons who have a "need to know" business purpose for FTI. For Covered California, the only persons with a "need to know" business purpose for FTI are those persons who will be doing appeal reviews. These staff members, and only these staff members, will be authorized to access FTI.

The IRS rules for access to FTI include:

- Only staff members with a "need to know" business purpose for FTI can access it
- Staff must have specific authorization before they access FTI
- Staff must complete privacy and security training before they access FTI and complete it annually thereafter

The IRS also requires Covered California to take special steps to guard FTI, in addition to the safeguards that are used with PII. These special steps include:

- FTI must never be left unattended
- FTI must be labeled as being "FTI" and must be tracked
- FTI must be protected with **two physical barriers:** it must be placed inside a secured perimeter and in a locked container or in a locked perimeter and secured interior, or in a locked perimeter and a security container
- Restricted access areas and special storage procedures for electronic FTI must be used to ensure that only authorized staff can access FTI

When FTI is no longer needed, it must be properly destroyed:

- Paper FTI must be put in confidential destruct bins
- Electronic and encrypted media must be destroyed using methods approved by Covered California's Information Security Officer

Covered California has adopted special procedures to ensure it meets the IRS rules. All requests for receipt of, distribution of and disposition of FTI, electronic and paper, will be documented and audit logs will be monitored.

The IRS will regularly conduct on-site reviews of Covered California's safeguards to ensure they are adequate to protect FTI. Covered California will conduct internal inspections to ensure that adequate safeguards and security measures are being maintained.

3.1.3. What are the Penalties for Improper Inspection or Disclosure of FTI?

FTI can be used only for an authorized purpose and only to the extent authorized. The penalties for unauthorized disclosures of FTI can be high:

- It is a violation for any person to willfully disclose FTI without authorization, to willfully print or publish in any manner not provided by law any FTI, or to willfully offer any item of material value in exchange for FTI and to receive FTI as a result of such solicitation;
- These violations are felony offenses, punishable by a fine up to $5,000 and by imprisonment up to 5 years, or both (26 U.S.C. 7213)

The penalties for unauthorized access to FTI are also high:

- It is unlawful for any person willfully to inspect FTI without authorization
- Such inspection is punishable upon conviction by a fine up to $1,000 or imprisonment up to one year, or both, together with the costs of prosecution (26 U.S.C. 7213A)

Civil action for damages: Any person who knowingly or negligently inspects or discloses FTI may also be subject to a civil suit for damages by the taxpayer whose records were seen or disclosed and be liable for $1,000 for each act of unauthorized inspection or disclosure, or the actual damages sustained by the taxpayer, whichever is greater (26 U.S.C. 7431)

3.1.4. Reporting any Violations or Suspected Violations of the Rules Regarding FTI

Covered California staff must follow the special rules and safeguards that apply to FTI. **REMEMBER**: only staff with special authorization is permitted to have access to FTI and only if they have a business need for FTI. If you become aware of any unauthorized access or disclosure of FTI, or if you have any reason to believe it may have happened or may be occurring, you must **IMMEDIATELY** report it to Covered California's Information Security Officer:

Phone: 916.539.4892
Email: InformationSecurity@covered.ca.gov

3.1.5. Lesson Activity 1

Test your PII IQ. For each statement, answer true or false.		
	True	**False**
PII stands for "personally identifiable information"		
Someone's driver's license is not PII.		
One way to protect PII is to use the full Social Security number of an individual.		
FTI stands for "federal tax information"		

Answers to this activity are at the end of this course.

4. LESSON 3: WHAT IS PROTECTED HEALTH INFORMATION (PHI)?

In this lesson you will learn the definition and rules regarding the use of Protected Health Information (PHI).

4.1. Learning Objectives

At the end of this lesson you will be able to:

- ✓ Define Protected Health Information (PHI)
- ✓ Describe the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Privacy Rule and Security Rule
- ✓ Describe individuals' rights regarding PHI

4.1.1. PROTECTED HEALTH INFORMATION (PHI)

Information is considered PHI if it is individually identifiable and:

- Relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present or future payment for health care
- Was created/received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse (e.g. a 3rd party medical biller)
- Includes documents in ANY medium: written, oral, or electronic

Examples of PHI Include:

- Information doctors, nurses and other healthcare professionals put in a patient's medical records
- Conversations a doctor has with nurses and other medical personnel about a patient's care or treatment
- Information about an individual that resides in their doctor and hospital's computer system
- Billing information about a patient

Information used in HIPAA transactions is considered individually identifiable if it can be linked to an individual. If any of the "identifiers" listed below are included, the information is usually considered individually identifiable and must be protected under HIPAA rules:

- Names
- Geographic subdivisions smaller than a State (including street, address, city, county, zip code)
- Dates (except year) for dates directly related to the individual (birth date, admission date, etc. and all ages over 89)
- Telephone numbers
- Fax numbers
- Electronic mail addresses
- Social security numbers
- Medical record numbers,
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers
- Device identifiers and serial numbers
- Web Universal Resources (URLs)
- Internet Protocol (IP) address numbers

- Biometric identifiers
- Full face photographic images
- Any other unique identifying number, characteristic or code

Please note: PHI can be in many forms including paper, CDs/ DVDs, flash drives, smart phones, and laptops.

4.1.2. INDIVIDUALS' RIGHTS

Individuals have many rights regarding their PHI, including the right to:

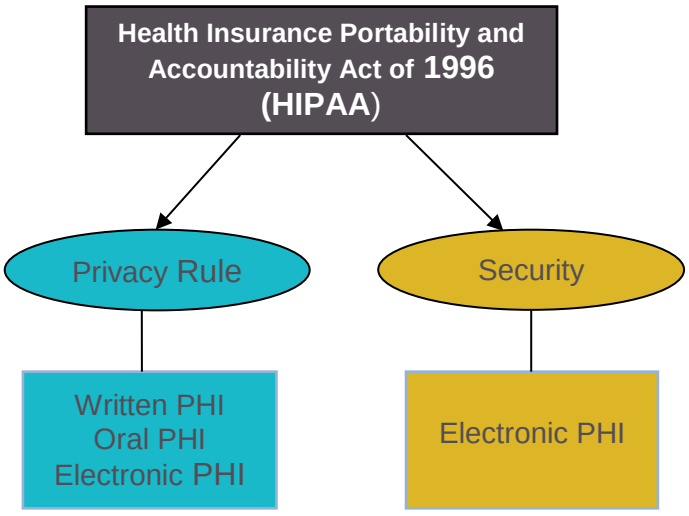
- Receive a copy of their health records
- Request confidential communications
- Request corrections to their health information
- Receive a Notice of Privacy Practices that tells them what their rights are and how their health information may be shared
- Request restrictions on how their health information is shared
- Get a report on when and why their health information was shared
- File complaints alleging their privacy rights were violated

As set out above in the discussion on the federal regulation, Covered California has implemented procedures so that individuals can exercise these rights. Forms for requesting a copy of records with personal information, confidential communications, corrections to records, restrictions on uses, and an accounting of disclosures are posted on the Covered California web site. A form for filing a complaint is also on the web site.

Covered California has also adopted a Notice of Privacy Practices, which sets out its privacy practices and the rights of individuals. The Notice is posted on the Covered California web site.

4.1.3. WHAT ARE THE PRIVACY AND SECURITY RULES?

PHI is protected under federal regulations known as the Privacy Rule and the Security Rule. These regulations were developed as a result of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and require privacy and security protections for individually identifiable health information. These HIPAA regulations are enforced by the U.S. Department of Health and Human Services (HHS), Office for Civil Rights (OCR).



The Privacy Rule covers ALL PHI, whether written, oral, or electronic and includes:

The use and disclosure of a person's individually identifiable health information by organizations subject to the Privacy Rule (covered entities)

The ability for individuals to understand and have more control over their health information and how it is used

The Security Rule protects an individual's electronic protected health information, or e-PHI. A major goal of the Security Rule is to allow covered entities to use new, more-efficient technologies to help improve the quality of consumer care and still protect the privacy of an individual's health information.

Let's Review the Two Rules:	Privacy Rule	Security Rule
Developed as a result of HIPAA	✓	✓
Protects written PHI	✓	
Protects oral PHI	✓	
Protects electronic e-PHI	✓	✓

4.1.4. WHO MUST FOLLOW THE PRIVACY AND SECURITY RULES?

Covered Entities

The entities that must follow the HIPAA regulations are called covered entities. Covered entities include health plans, health care clearinghouses and health care providers.

- Health plans include health insurance companies that provide or pay for the cost of medical care through a health plan, such as HMOs, company health plans and government health programs that pay for health care such as Medicare, Medi-Cal and military and veterans' health care programs.
- Health care clearinghouses are entities such as billing services, re-pricing companies, and community health management information systems that put nonstandard health information into a standard format or data content.
- Health care providers include any person or organization that provides, bills, or is paid for health care in the normal course of business, such as doctors, hospitals, nursing homes, clinics and pharmacies; these providers are covered entities if they transmit health information in electronic form to conduct transactions that are covered by HIPAA, such as electronically billing a health insurance company.

Business Associates

A business associate performs work for a covered entity that involves using or disclosing the covered entity's PHI. A business associate may be a contractor, subcontractor or vendor working for the covered entity, and can itself be a covered entity. Under the HIPAA rules, the covered entity using the services of a business associate must have a written agreement with the business associate that requires the business associate to follow HIPAA privacy and security rules when it performs work involving the covered entity's PHI. The business associate can only use the PHI for the purpose for which the covered entity

shares it. Doctors, hospitals, health insurance companies and some governmental agencies may use business associates to carry out some of their functions.

Definition of Business Associate	Examples of Business Associates
A person or entity that performs certain functions or activities that involve the use or disclosure of PHI on behalf of, or that provides services to, a covered entity.	An independent medical transcriptionist that provides transcription services to a doctor A third-party administrator that assists a health insurance company with claims processing A CPA firm whose accounting services involve access to PHI

4.1.5. WHEN CAN PHI BE USED AND DISCLOSED?

Permitted Uses and Disclosures

A covered entity is permitted (but not required) to use and disclose PHI without an individual's authorization in the following situations:

- To the individual who is the subject of the PHI
- Treatment, payment, and health care operations activities such as doctor and hospital or health insurance company performance evaluations, audits, medical reviews, accreditation, business planning, de-identifying PHI, etc.
- Opportunity to agree or object. Informal permission may be obtained by asking the individual outright
- Incident to an otherwise permitted use and disclosure. In this case, the PHI disclosed is related to PHI that has already been given permission to be used and disclosed
- Public interest and benefit situations. There are 12 national priority purposes when PHI can be disclosed without an individual's authorization; for example, with victims of abuse, judicial proceedings, and law enforcement purposes
- Limited data set. In this case, direct identifiers have been removed from the PHI and it can now be used for research, health care operations, and public health purposes

***Ask your supervisor for permission before using or disclosing PHI**

Required Uses and Disclosures

A covered entity is *required* to disclose PHI in only two situations:

- To individuals when they request access to, or an accounting of disclosures of, their PHI
- To HHS when it is investigating the covered entity or determining its compliance with HIPAA

Authorized Uses and Disclosures

A covered entity must obtain the individual's written authorization for any use or disclosure of PHI that is not for treatment, payment, or health care operations or otherwise permitted or required by the Privacy Rule. Examples of disclosures that would require an individual's written authorization include:

- Disclosures to a life insurer for coverage purposes
- Disclosures to an employer of the results of a pre-employment physical or lab test
- Disclosures to a pharmaceutical firm for their own marketing purposes

The Principle of "Minimum Necessary" Use and Disclosure

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 necessary amount of PHI needed for an intended purpose. The minimum necessary requirements do not apply to the following:

- Disclosures to or requests by a doctor or hospital for treatment purposes
- Disclosures to the individual who is the subject of the information
- Uses or disclosures with an individual's authorization
- Uses or disclosures required for HIPAA standard transactions
- Disclosures to HHS when the disclosure of information is required under the Privacy Rule for enforcement purposes
- Uses/disclosures required by law

4.1.6. Safeguards and the Privacy Rule

The safeguards requirement in the Privacy Rule establishes protections for all PHI, regardless of form (paper, oral, or electronic). There are three types of safeguards: administrative, technical, and physical. HIPAA requires all covered entities to have these safeguards in place to protect the privacy of PHI. They are used to maintain the confidentiality, integrity, and availability of PHI, as well as to prevent unauthorized or inappropriate access, use, or disclosure. These safeguards will be described in a later lesson in this course.

4.1.7. Filing Complaints

Anyone can file a complaint alleging a violation of the Privacy Rule or Security Rule. If a consumer believes that a covered entity violated their health information privacy rights, they can file a complaint with the Office for Civil Rights (OCR) or to HHS. Under HIPAA, an entity cannot retaliate against a consumer for filing a complaint.

There are two ways to file a complaint with the OCR:

1. A consumer may use the OCR Health Information Privacy Complaint Form Package. It is available online at: http://www.hhs.gov/ocr/privacy/hipaa/complaints/hipcomplaintpackage.pdf
2. Consumers may submit a written complaint in their own format, including the following information:
   - Full name

- Full address
- Telephone numbers
- E-mail address (if available)
- Name, full address, and telephone number of the person, agency, or organization believed to have violated their health information privacy rights or committed another violation of the Privacy Rule or Security Rule
- Brief description of what happened: how, why, and when they believe their health information privacy rights were violated, or how the Privacy Rule or Security Rule was otherwise violated
- Any other relevant information
- Signature and date of complaint

The complaint should be mailed or faxed to the appropriate OCR regional office (based on where the alleged violation took place).

Locations and fax numbers can be found online at:
http://www.hhs.gov/ocr/office/about/rgn-hqaddresses.html
or
E-mail: OCRComplaint@hhs.gov

Note: The complaint should be filed within 180 days of the Privacy Rule or Security Rule violation.

4.1.8. LESSON ACTIVITY 2

in
Fill in the blanks.

1. Entities that must follow the Privacy and Security Rules are called _____ entities.

2. Information that is used in a HIPAA transaction and is individually identifiable is called _____ _____ _____

3. There are only _____ circumstances when a covered entity is required to disclose information that is protected under HIPAA.

4.1.9. LESSON ACTIVITY 3

Fill in the blanks.

1. A central aspect of the Privacy Rule is the principle of _____ _____use and disclosure.

2. A covered entity must obtain _____ _____from an individual for any use or disclosure of PHI that is not for treatment, payment, or health care operations permitted or required by the Privacy Rule.

3. When a covered entity can use and disclose an individual's PHI it is called a _____ use and disclosure.

5. LESSON 4: INCREASING INFORMATION SECURITY AWARENESS

In this lesson you will learn ways in which you can increase information security awareness such as: protecting your workplace and equipment, safeguarding e-mails, avoiding computer security risks like viruses and malware and practice safe social media use.

5.1. LEARNING OBJECTIVES

At the end of this lesson you will be able to:

- ✓ Define ways to select and keep your passwords safe
- ✓ Identify ways to keep mobile devices and laptops secure
- ✓ Identify methods for maintaining security while working remotely
- ✓ Identify ways to avoid common email security safeguards
- ✓ Identify the importance of Malware/Virus protection
- ✓ Define Phishing Security Guidelines
- ✓ Define Social Engineering Security Guidelines
- ✓ Identify ways to protect yourself when using social media

5.1.1. INFORMATION SECURITY SAFEGUARDS FOR PROTECTING COVERED CALIFORNIA

Safeguards and the Security Rule

As with the Privacy Rule, the Security Rule also requires adherence to appropriate administrative, technical, and physical safeguards.

- ***Administrative*** safeguards are administrative actions, policies, and procedures to manage the selection, development, implementation, and maintenance of security measures to protect data and to manage the conduct of the Covered California's workforce in relation to the protection of that information.
- ***Physical*** safeguards are physical measures, policies, and procedures to protect Covered California's electronic information systems and related buildings and equipment, from natural and environmental hazards and unauthorized intrusion.
- ***Technical*** safeguards mean the technology and the policy and procedures for its use that protect information system data and control access to it.

Examples of Required Security Rule Safeguards		
ADMINISTRATIVE[1]	**TECHNICAL**[2]	**PHYSICAL**[3]
• Implement policies and procedures to prevent, detect, contain, and correct security violations. • Conduct an accurate and thorough assessment of the	• Implement technical policies and procedures for electronic information systems that maintain data to allow access only to those persons that have been	• Implement policies and procedures to limit physical access to electronic information systems, while ensuring that properly authorized access is allowed. • Implement policies and

Examples of Required Security Rule Safeguards		
ADMINISTRATIVE[1]	**TECHNICAL**[2]	**PHYSICAL**[3]
potential risks and vulnerabilities to the confidentiality, integrity, and availability of data held by Covered California. • Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with risk management. • Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the Covered California. • Implement policies and procedures to ensure all members of the workforce that require access have appropriate access to data and to prevent those that do not require access from obtaining access to data. • Identify the security official responsible for the development and implementation of the required policies and procedures. • Implement a security awareness and training program for all members of the workforce. • Implement procedures	granted access rights. • Assign a unique name and/or number for identifying and tracking user identity. • Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use data. • Implement policies and procedures to protect data from improper alteration or destruction. • Implement procedures to verify the authenticity of a person or entity seeking access to e-PHI. • Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity. • Implement a mechanism to encrypt and decrypt data whenever deemed appropriate. • Implement technical security measures to guard against unauthorized access data that is being transmitted over an electronic communications	procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft. • Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision. • Implement physical safeguards for all workstations that can access data to restrict access to authorized users only. Keep laptop computers containing data to remain in your immediate physical possession or locked in a secure place. Do not leave laptops containing sensitive data in your car. • Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain data into and out of a facility, and movement within the facility. • Implement policies and procedures to address the final disposition of data. • Implement procedures

Examples of Required Security Rule Safeguards		
ADMINISTRATIVE[1]	**TECHNICAL**[2]	**PHYSICAL**[3]
for the authorization and/or supervision of Covered California users who work with sensitive data. • Implement procedures for terminating access to data when the employment of a user ends or is no longer required. • Implement policies and procedures that modify a user's access level when the level of access required changes • Implement policies and procedures to address security incidents. • Establish policies and procedures for responding to an emergency or other occurrence (for example: fire, vandalism, system failure, and natural disaster) that damages systems that contain sensitive data.	network. • Implement security measures to ensure that electronically transmitted e-PHI is not improperly modified without detection until disposed of.	for removal of data from electronic media before the media are made available to re-use.

5.1.2. KEEPING YOUR PASSWORDS SAFE

One of the best ways to keep information secure is to create strong passwords. Some examples of guidelines to create strong passwords include:

- The best passwords use a combination of numbers, upper and lowercase letters and keyboard characters such as: * & $
- Passwords should be at least 8 characters
- If possible, do not use only letters or only numbers
- Do not use names of family members
- Do not leave the password blank

- A good password is easy to remember but hard to guess
- Consider using the first letter of the words in a phrase or song.

Example:

"Mary had a little lamb, little lamb, little lamb" would equal "Mhall,ll,ll."

"To be or not to be" would equal "2bon2b"

Guidelines for keeping your passwords safe

It is not only important create strong passwords; you must also practice behaviors that will keep your password safe. Some of these behaviors include:

- Do not write down your password
- Do not share your password with others
- Do not reuse passwords
- Using the same password for multiple different sites and devices can lead to identity theft
- Change password every 30 to 60 days
- Avoid reusing the same password for at least a year

Note: Report any suspected unauthorized use of your user ID or password immediately to your supervisor.

5.1.3. PROTECTING YOUR WORKSTATION, LAPTOP AND MOBILE DEVICE

Protecting your workstation

Securing Information when you leave your PC/Workstation is critical to maintain information security. Here are some practices that will help safeguard information while stepping away from your desk:

- Always log off of desktops, laptops and any portable electronic devices that have network access, such as a smart phone.
- Ensure paper documents are secure at all times. Lock your workstation when not in use.
- Make sure your workstation screen is not visible to the public.
- Use only computers, networks, applications and information for which you are authorized.

Covered California reserves the right to limit, restrict or extend access to its computer network and to its data resources.

Another aspect of information security to be mindful of is the potential of outside intruders entering the work area. Some common intrusion tactics to be aware of are:

- Unauthorized physical access
- Shoulder surfing
- Impersonation on help desk calls
- Wandering through halls looking for open offices

- Stealing sensitive documents

Protecting your mobile device/laptop

Mobile devices (smart phones, laptops) often contain sensitive information. You are responsible for the confidentiality/security of your mobile devices. If your mobile device is lost or stolen and contains sensitive information, you must report it to your supervisor and Covered California. There are many ways in which you can better secure your mobile device:

- Turn off Bluetooth discovery mode
- Avoid Wi-Fi hotspots
- Beware of text message spam
- Be careful with smart phone applications
- Avoid location "check-ins”
- Do not store passwords on the phone
- Turn off geotagging, or turn off photo auto-uploads
- If you lose/misplace your smart phone, use the "remote location" feature
- Download security updates and back-up your data regularly

There are many ways in which you can better protect your laptop:

- Always use a docking station or laptop security cable
- Keep information secure on your laptop
- Data Encryption
- Virus Protection
- Symantec Endpoint Protection
- Antivirus application

5.1.4. SECURITY WHILE TRAVELING AND WORKING REMOTELY

While our mobile devices and laptops give us great freedom, they also come with special security issues. Here is a list of safeguards to help increase security while traveling and working remotely:

- Avoid using computer bags
- Use strong passwords, and do not keep them in your laptop/tablet bag
- Encrypt your data
- Carry your laptop with you
- Keep an eye on your laptop/tablet
- Avoid setting your laptop/tablet on the floor
- Try not to leave your laptop/tablet in your hotel room
- Use a laptop security cable
- Affix your name and contact info to laptops/tablets

- Turn off your laptop's Wi-Fi capability when you are not using it
- Use a Virtual Private Network (VPN)
- Disable file and printer sharing
- Make your folders private
- Use a personal firewall
- Consider removing sensitive data from your portable computer
- Use anti-virus software and keep it updated

5.1.5. E-MAIL SECURITY

When using e-mail, slow down, think and check before hitting send. Common mistakes include:

- Auto-complete: E-mail systems complete addresses before you finish typing. Always verify the name and the e-mail address before you hit Send.
- Copying and blind copying (cc/bcc): Take a look at who is on the "cc" list and "Bcc" list. If your reply is sensitive in nature, you may want to reply only to the sender.

The Do's and Do Not's of E-mail Security of Knowledge

Do's	Do Not's
Open e-mails only from people you know and trust.	Do not provide your e-mail or someone else's e-mail address online.
Open only those e-mail attachments whose headings or texts sound familiar.	Do not trust a site just because it claims to be secure.
Use e-mail encryption for particularly sensitive messages.	Do not open e-mail attachments from unfamiliar sources.
Delete suspicious messages	Do not open e-mail attachments containing the following file extensions: .exe, .bat, .reg, .scr, .dll, or .pif.
Check out the website uses before sending any sensitive information.	Do not reveal your credit card number or other sensitive information by e-mail.
	Do not provide personal information, unless you are certain of a person or organization's authority to ask for it.
	Do not open e-mails addressed to people other than you.
	Do not respond to e-mails that request your personal or financial information.

5.1.6. PAYMENT CARD SECURITY

Avoid violating payment card industry security standards by adhering to the following rules:

- Do not store cardholder data unless it is absolutely necessary.
- Retain (if you have a legitimate business need) cardholder data only if authorized, and ensure it is protected.
- Do not store sensitive authentication data contained in a payment card's chip.
- Do not permit unauthorized people to access stored cardholder data.
- Do not put paper containing credit card data in the regular trash.
- Do not e-mail or instant message credit card numbers.
- Never store full contents of any track from the card's magnetic stripe or chip.
- Never store the personal identification number (PIN) or PIN Block.

Do not betray your customers' trust. Protect every credit card number as though it were your own.

5.1.7. COMPUTER SECURITY: VIRUSES, MALWARE AND PHISHING

It is important to practice safe behaviors when operating your computer to avoid viruses, malware and phishing scams. There are thousands of types of malicious software, also known as malware. Some examples include:

- Viruses
- Worms
- Spyware
- Trojan horses
- Rogue security software

A computer virus is a computer program with malicious intent. It can be hidden in pirated software, in files or programs that you might download. It is not always easy to tell if your computer has been infected, listed here are some signs that show that your system might possibly be infected:

- Your computer runs more slowly than normal.
- Your computer stops responding or freezes often.
- Your computer crashes and restarts every few minutes.
- Your computer restarts by itself and then fails to run normally.
- You see distorted menus and dialog boxes.
- Applications on your computer don't work correctly.
- Disks or disk drives are inaccessible.
- You cannot print correctly.
- You see unusual error messages.

Another potential problem is rogue software. A rogue security software program tries to make you think that your computer is infected by a virus and usually prompts you to download or buy a product that removes the virus.

- Do not be fooled! If the error message does not come from your antivirus application, do not click “OK” to download.
- Report all virus/malware infections to your supervisor

Phishing is a form of online scam that attempts to collect personal and financial information. It may look quite authentic, featuring corporate logos and formats similar to the ones used for legitimate messages. Results can range from account closures to financial ruin, and in the worst cases, identity theft. Phishing E-mails typically contain:

- A generic greeting
- Warning of a sudden change in an account that requires entering private information to correct
- Poor spelling or grammar

Here are some ways to avoid phishing schemes:

- Question impersonal e-mails
- Be wary of requests for confidential information
- Question the “scare tactic” message
- Do not reply to any e-mail asking to verify your personal data
- Make sure you are on a secure web server when submitting credit card or other sensitive information, via your web browser
- Notify your supervisor immediately if you receive a phishing scam, notice strange behavior on your computer, or if unexpected software is running

5.1.8. SOCIAL MEDIA SAFETY

Social media sources are services people use to connect with others to share personal information. Some of the most common examples include the following:

- Facebook
- Twitter
- Instagram
- Pinterest

The security issue with social networking is that hackers, spammers, virus writers, identity thieves and other criminals follow the traffic on these sites. As social media usage grows so does the need to keep identities secure.

Tips for social media protection:

- Create a social specific e-mail.
- Do not use your Covered California e-mail account ID/password
- Use discretion before posting anything online.
- Know what you have posted about yourself.

- Do not trust that a message is really from who it says it is from.
- Do not allow social networking services to scan your address book.
- Be selective about who you accept as a friend on a social network.
- Use a strong password.
- Remember: downloading videos increases susceptibility to viruses

Social engineering is the art of manipulating people so they give up confidential information. Attackers use e-mail, social networks, and phone contacts to reach their victims. Tips to protect you from social engineering include:

- Be suspicious of unsolicited phone calls, visits or e-mail messages.
- Do not reveal personal or financial information in e-mails or follow links sent in suspicious e-mails.
- If the message conveys a sense of urgency, be skeptical.
- Dumpster diving, also known as “trashing,” is another popular method of social engineering.
- The internet is where social engineers look to harvest passwords.
- The most prevalent type of social engineering attack is conducted by phone.

5.1.9. LESSON ACTIVITY 4

Test your knowledge on workstation, mobile devices, and laptops.

	True	False
A secure password should be five alphabet letters or less.		
You should write down your passwords so you do not forget them.		
When you leave your workstation, you should log off or lock your workstation.		
Store your passwords on your smart phone so you do not forget them.		
If you see a good software program, install it on your laptop.		

5.1.10. LESSON ACTIVITY 5

Test your knowledge on safety while traveling and working remotely.

	True	False
When working remotely, you should carry your laptop/tablet in a computer bag.		
Don’t put your name or contact information on the laptop/tablet.		
Disable file and printer sharing so that you are less vulnerable to hackers.		
If you leave your laptop/tablet in your hotel room, use a security cable to secure the laptop.		

5.1.11. LESSON ACTIVITY 6

Fill in the blanks.

1. Open only those e-mail attachments whose headings or texts sound_____.
2. When using e-mail, slow down, _____, and check before hitting send.
3. Do not send_____ information over the internet before checking the website security.
4. Do not open attachments to e-mails from _____sources.

5.1.12. LESSON ACTIVITY 7

Fill in the blanks.

1. Your computer may be infected with a virus if it runs more _____.
2. To protect against computer viruses, do not _____ on attachment files whose names end with .nws.
3. Some rogue security software might install _____ to steal your data.
4. Any communication that begins with “Dear Bank of America Customer” ought to signal_____.
5. Be wary of requests for _____ information.

5.1.13. LESSON ACTIVITY 8

Test your knowledge on safety while traveling and working remotely.

	True	False
If you receive an unsolicited phone call, asking for information about Covered California, such as networks, you should reveal this information.		
If the message conveys a sense of urgency, you should act quickly.		
The most prevalent type of social engineering attack is conducted by phone.		
A common social engineering tactic is impersonation on help desk calls.		

6. LESSON 5: PENALTIES FOR VIOLATIONS OF PRIVACY LAWS

The federal and state privacy laws and regulations that protect confidential information collected, used and disclosed by Covered California provide various penalties if this information is improperly used or disclosed. Some of these penalties are quite severe. Improper use or disclosure can also expose the individual who improperly uses or discloses PII to personal civil liability. These penalties and consequences are set out below in this lesson.

6.1. LEARNING OBJECTIVES

At the end of this lesson you will be able to:

- ✓ Describe the penalties under the federal regulation
- ✓ Describe the penalties under the IPA
- ✓ Describe the penalties under IRS rules
- ✓ Describe the penalties under HIPAA
- ✓ Describe the penalties under the California Penal Code
- ✓ Describe employee sanctions

6.1.1. PENALTIES UNDER THE AFFORDABLE CARE ACT, 45, C.F.R. 155.260

Under the Affordable Care Act (ACA), information provided by applicants may be used only for the purposes of, and to the extent necessary in, ensuring the efficient operation of the Exchange, and shall not be disclosed to any other person except as provided in the applicable section of the ACA (42 U.S.C. 18081(g).)

If applicant information is disclosed in violation of this section, the following penalty applies:

- Knowingly and willfully use or disclose information in violation of this section
- Civil penalty of not more than $25,000 per person or entity, per use or disclosure, in addition to other penalties that may be prescribed by laws (45 C.F.R. 155.260(g).)

6.1.2. PENALTIES UNDER THE STATE INFORMATION PRACTICES ACT (IPA)

The State Information Practices Act (IPA) imposes the following criminal penalties:

- To willfully request or obtain any record with personal information from an agency under false pretenses is a misdemeanor, punishable by a fine not more than $5,0000 or imprisonment not more than one year, or both (Calif. Civil Code, section 1798.56)
- Intentional disclosure of medical, psychiatric or psychological information is a misdemeanor if the wrongful disclosure results in economic loss or personal injury to the individual to whom the information pertains (Calif. Civil Code, section 1798.57)

Civil action: Any person, other than an employee, who intentionally discloses non-public information, which they know or should reasonably know, came from a state agency may also be subject to a civil action for invasion of privacy. In additional to general damages, a minimum of $25,000 may be imposed as exemplary damages, plus attorney fees and costs (Calif. Civil Code, section 1798.53).

6.1.3. PENALTIES UNDER IRS RULES

FTI can be used only for an authorized purpose and only to the extent authorized. The penalties for unauthorized disclosures of FTI can be high:

- It is a violation for any person to willfully disclose FTI without authorization, to willfully print or publish in any manner not provided by law any FTI, or to willfully offer any item of material value in exchange for FTI and to receive FTI as a result of such solicitation;

- These violations are felony offenses, punishable by a fine up to $5,000 and by imprisonment up to 5 years, or both (26 U.S.C. 7213)

The criminal penalties for unauthorized access to FTI are also high:

- It is unlawful for any person willfully to inspect FTI without authorization
- Such inspection is punishable upon conviction by a fine up to $1,000 or imprisonment up to one year, or both, together with the costs of prosecution (26 U.S.C. 7213A)

Civil action for damages: Any person who knowingly or negligently inspects or discloses FTI may also be subject to a civil suit for damages by the taxpayer whose records were seen or disclosed and be liable for $1,000 for each act of unauthorized inspection or disclosure, or the actual damages sustained by the taxpayer, whichever is greater (26 U.S.C. 7431)

6.1.4. HIPAA Penalties for Covered Entities and Business Associates

Under HIPAA, civil money penalties may be imposed upon both covered entities and business associates for violations of the HIPAA rules. The penalties are progressive and a minimum penalty may be imposed even if the covered entity did not know of the violation:

- For violations where the covered entity did not know and, by exercising reasonable diligence, would not have known, of the violation:
  - Minimum penalty of $100 per violation
  - Maximum penalty of $50,000 per violation
- For violations due to reasonable cause and not willful neglect:
  - Minimum penalty of $1,000 per violation
  - Maximum penalty of $50,000 per violation
- For violations due to willful neglect, but the violation is corrected within 30 days after the covered entity knew or should have known of the violation:
  - Minimum penalty of $10,000 per violation
  - Maximum penalty of $50,000 per violation
- For violations due to willful neglect and not corrected:
  - Penalty of $50,000 per violation
- For each tier of penalties, there is a maximum penalty of $1.5 million that may be imposed for identical violations within a calendar year

There are also criminal sanctions under HIPAA that can be imposed on covered entities:

- For knowingly obtaining or disclosing PHI in violation of the HIPAA rules, the penalties include a fine up to $50,000 and imprisonment up to one year
- If the offense is committed under false pretenses, the penalties include a fine up to $100,000 and imprisonment up to five years
- If the offense is committed with the intent to sell, transfer or use PHI for commercial advantage, personal gain or malicious harm, the penalties include a fine up to $250,000 and imprisonment up to 10 years

6.1.5. California Penal Code Penalties

The California Penal Code makes it a crime to:

- Knowingly access and without permission alter, damage, delete, destroy or otherwise use any data, computer, computer system, or computer network to commit fraud or to wrongfully control or obtain money, property or data
- Knowingly access and without permission take, copy or make use of any data from a computer, computer system, or computer network, or take or copy any supporting documentation
- Knowingly access and without permission add, alter, damage, delete or destroy any data, computer, software or computer programs
- Knowingly and without permission disrupt or cause the disruption of computer services or deny or cause the denial of computer services to an authorized user of a computer, computer system or computer network
- These offenses are punishable by a fine up to $10,000, imprisonment up to three years or both fine and imprisonment. (Calif. Penal C., § 502(c)(1), (2), (4) and (5), and (d).)The Penal code also defines lesser offense that are punishable by fine and imprisonment in county jail.

6.1.6. Employees

Any state employee who violates Covered California's privacy or security policies or procedures will be subject to the State Progressive Discipline Process.

In addition, under the IPA, the intentional violation of the IPA by an officer or employee of any state agency shall constitute a cause for discipline, including termination of employment. (Civil Code section 1798.55)

7. LESSON 6: REPORTING PRIVACY AND SECURITY INCIDENTS

This lesson focuses on the importance of reporting any suspected or actual incidents to protect Covered California's confidential information, data systems, services and networks. Diligence and immediacy in reporting is required to maintain privacy and security in Covered California.

7.1. LEARNING OBJECTIVES

At the end of this lesson you will be able to:

- ✓ Identify a security incident
- ✓ Identify a privacy incident
- ✓ Know how to report a security or privacy incident
- ✓ Understand the importance of immediate action to detect and report incidents

7.1.1. Duty to Detect and Report Incidents

All Covered California staff and all contractors and vendors who have access to Covered California data systems, services or networks, or access to any confidential information (PII, FTI, PHI) that is collected, maintained, used or disclosed by Covered California, must

immediately report any incident that may affect the confidentiality, security or integrity of the data or the systems.

- This includes suspected incidents. You should not wait to confirm the incident happened, or to investigate what happened, but must immediately report any suspected incident.
- When you report an incident, Covered California Information Security Office staff can then take immediate actions to prevent harm and will direct you on what actions you need to take.
- The duty to report includes both security incidents and privacy incidents.

7.1.2. SECURITY INCIDENTS

A Security Incident is defined as:

> Any real or potential attempt (successful or unsuccessful) to access and/or adversely affect Covered California data, systems, services or networks, including CalHEERS data, systems, services and networks, and including but not limited to any effect on data availability, loss of data, disclosure of proprietary information, illegal access and misuse or escalation of authorized access.

Examples of security incidents include, but are not limited to:

- **Denial of Service** – an attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources
- **Malicious Code** – a virus, worm, Trojan horse, or other code-based malicious entity that successfully infects a host
- **Unauthorized Wireless Devices Detection** – connecting an unauthorized wireless access point into a Covered California computer system
- **Unauthorized Access** – a person gains logical or physical access without permission to a network, system, application, data, or other IT resource
- **Inappropriate Usage** – a person violates acceptable use of any network or computer policies
- **Lost or Stolen Asset** – a Covered California or CALHEERS asset is lost or stolen or personal belongings of a Covered California employee or contractor are stolen at a work location

7.1.3. PRIVACY INCIDENTS

A Privacy Incident is defined as:

> The attempted or successful unauthorized access, use, disclosure, modification or destruction of Personally Identifiable Information (PII), Protected Health Information (PHI) or Federal Tax Information (FTI) or interference with system operations in an information system that processes, maintains or stores PII, PHI or FTI.

Examples of privacy incidents include, but are not limited to:

- **Fax** – papers with PII are sent to the wrong fax number
- **Mail** – a package containing papers with PII and PHI is mailed using standard U.S. postal service methods, but it arrives damaged and some papers may be missing or may have been seen by unauthorized persons
- **Oral** – two employees discuss confidential application information in a lobby area, where other people walk through and can overhear them
- **Public posting** – a list of service center representatives with their service center contact information is posted on a public website, but the list inadvertently contains their home addresses, phone numbers and names of their dependents
  Unauthorized access – a computer file with personal information on applicants, including income information, is sent to the wrong vendor who uploads it to the vendor's computer system and the file is accessed by the vendor's employees
- **Unauthorized use and access** – an employee wants to work at home to catch up on a backlog so sends files with applicants' personal information to his/her home computer, where a visiting nephew views the file when the employee opens it
- **Minimum necessary violation** – an employee needs to verify what information was received on a specific application, so downloads all applications received that day to make it easier to skim through them, looking for the one application that is needed

7.1.4. Reporting Security and Privacy Incidents

You must IMMEDIATELY REPORT a suspected or actual security or privacy incident to:

Your supervisor
Email: InformationSecurity@covered.ca.gov
Telephone: 916.539.4892

The Information Security Office monitors the email and telephone number several times a day and will respond to all reports of incidents. They will send you an Incident Report Form to fill out, which will ask for basic information about the incident. The Information Security Office staff will alert the Privacy Officer and other executive staff of the incident as needed and will forward reports to them. Either the Information Security Officer or the Privacy Officer will direct you on the next steps to be taken.

7.1.5. Immediate Action is Critical

Based upon the information they receive, the Information Security Officer and Privacy Officer will direct an investigation, determine what immediate action is needed, and develop a plan to identify gaps and to take corrective actions to prevent a future re-occurrence of a similar incident.

- Prompt action may mitigate harm by stopping continued inappropriate access to PII, PHI or FTI. For example, if personal information has been publicly posted, it can be removed and the persons whose information was exposed can be notified so that they can take steps to protect themselves.
- Further damage may be prevented by taking immediate steps to end unauthorized use or access. For example, if an electronic file with personal information has been sent to the wrong vendor, it can be identified and removed before anyone accesses it

Your diligence in immediately reporting any suspected or actual incident is essential to keep Covered California's confidential information and its data systems, services and networks safe and protected. With your help, Covered California can keep its confidential information and systems secure.

8. ANSWERS

Activity 1

Answers:

1. True
2. False
3. False
4. True

Activity 2

Answers:

1. Covered
2. Protected Health Information
3. Two

Activity 3

Answers:

1. Minimum & Necessary
2. Written authorization
3. Limited Data Set
4. Permitted

Activity 4

Answers:

1. False
2. False
3. True
4. False
5. False

Activity 5

Answers:

1. False
2. False
3. True
4. True

Activity 6

Answers:

1. Familiar
2. Think
3. Sensitive
4. Unfamiliar

Activity 7

Answers:

1. Slowly
2. Click
3. Malware
4. Phishing
5. Personal

Activity 8

Answers:

1. True
2. False
3. True
4. False

9. ENDNOTES

[11] Source: 45 CFR §164.308

[12] Source: 45 CFR §164.312

[13] Source: 45 CFR §164.310