COVERED CALIFORNIA

Privacy, Security and Compliance

Participant Guide

Version 3.0

TABLE OF CONTENTS

1. Course Objectives

- ✓ Define PII, FTI and PHI and understand their appropriate use
- ✓ Identify the professional conduct and ethics expected of people who work with Covered California
- ✓ Identify applicable Covered California policies and procedures
- ✓ Know how to protect confidential information
- ✓ Identify different types of conflicts of interest, learn on how to avoid them, deal with them and report them
- ✓ Demonstrate why preventing fraud, waste and abuse is important
- ✓ Report privacy, security and compliance violations

2. What Is Personally Identifiable Information (PII)?

What is PII?

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

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

Federal PII

The Code of Federal Regulations (CFR) under the Affordable Care Act describes privacy and security requirements for PII in health exchanges, such as Covered California, and can be found in the 45 C.F.R. 155.260. These regulations require Covered California to safeguard the PII it collects, maintains and uses so that no one unauthorized to access or use the PII can do so. Covered California must also protect the integrity of PII so that it cannot be altered or destroyed by an unauthorized user. The regulations also limit Covered California to use and disclose only 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 way to access and obtain their PII in a readable form and format

- ***Correction*** - Consumers should be provided with a timely way to dispute the accuracy or integrity of their PII, to correct erroneous information and the opportunity 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 their PII
- ***Individual Choice*** - Consumers should be provided a reasonable opportunity and the 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 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 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 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 adhered to through stringent monitoring. Other means and methods should be in place to report and mitigate non-adherence and breaches

INDIVIDUALS' RIGHTS

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

- To request a copy of records with their personal information, or to inspect the records
- To request correction of records of personal information
- To request restrictions on the use and disclosure of their personal information
- To request confidential communications, so that communications to the individual are sent to the address the individual chooses
- To request an accounting of disclosures, showing the date, nature and purpose of disclosure of personal information to other entities
- To file a complaint directly with Covered California, alleging Covered California violated privacy rules

These requests can be made by the individual or their personal representative by submitting a written request on the appropriate form. The forms are posted on CoveredCA.com on the Notice of Privacy Practices page.

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 they maintain that identifies or describes an individual. Personal information includes:

- Name

- Social Security Number
- Physical description
- Home address
- Home telephone number
- Education
- Financial data
- 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 limits must be placed on how the information is obtained and distributed to protect the individual
- ***Collecting Information*** - State agencies are required to collect only information that is relevant to the purpose of the agency and if possible to obtain that information from the individual rather than a secondhand source
- ***Disclosure*** - 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. However, if permission for disclosure is provided by an individual the information still must be kept secure

Important Note

You may be asked to upload personal information on behalf of the consumer during the enrollment/application process. This information should never be stored. Copies (either physical or electronic) must be deleted, destroyed or returned to the consumer immediately after use.

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

- To inspect their records, which are kept by the state agency and to get a copy of them
- To ask the agency to correct or remove information that they believe to be erroneous or irrelevant
- To see the agency's accounting of disclosures, which shows who has received the individual's records

Forms for requesting a copy of records with personal information, corrections to the records, and an accounting of disclosures are posted on the Notice of Privacy Practices page on CoveredCA.com.

SAFEGUARDING PII

Safeguarding PII prevents unpermitted disclosure and protects the integrity of the information by preventing unauthorized users from modifying or destroying it. PII should **NEVER** be sent via email, this includes screenshots from CoveredCA.com containing PII.

3. What Is Protected Health Information (PHI)?

Protected Health Information (PHI)

Information is considered protected health information (PHI) if it is individually identifiable health related information that:

- 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 third party medical biller)
- Includes content in ANY format or mechanism, including written, oral, or electronic

Examples of PHI Include:

- Information doctors, nurses and other health care 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's or 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:

- Name
- Geographic subdivision smaller than a state (including street address, city, county, zip code)
- Dates identifiable to an individual (birth date, admission date, etc.)
- Telephone number
- Fax number
- Electronic mail (email) address
- Social Security Number
- Medical record number
- Health plan beneficiary number
- Account number
- Certificate/license number
- Vehicle identifiers and serial number
- Device identifiers and serial number
- Internet Protocol (IP) address number and Web Universal Resource (URL)

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

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

INDIVIDUALS' RIGHTS

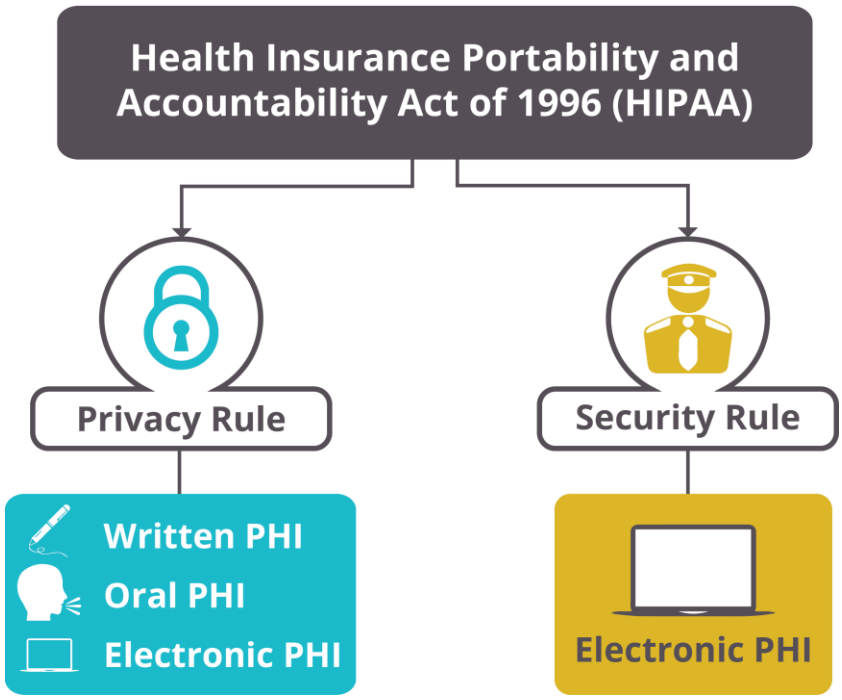
Individuals have many rights regarding their PHI, including the right to:

- 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 a complaint alleging their privacy rights were violated

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 Notice of Privacy Practices page on CoveredCA.com. A form for filing a complaint is also available on the website.

WHAT IS THE PRIVACY RULE AND SECURITY RULE?

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 (i.e. electronic patient charts) and still protect the privacy of an individual's health information.

	Privacy Rule	Security Rule
Developed as a result of HIPAA	✓	✓
Protects written PHI	✓	
Protects oral PHI	✓	
Protects electronic e-PHI	✓	✓

WHO MUST FOLLOW THE PRIVACY RULE AND SECURITY RULE?

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 an entity that involves using or disclosing the individual PHI. A business associate may be an employee, contractor, subcontractor or vendor working for a covered entity, and can itself be a covered entity.

Important

All certified in-person assistance personnel who work on behalf of Covered California, are considered business associates. You are required to follow all Covered California privacy and security requirements as described within this course.

Under the HIPAA rules, the covered entity using the services of a business associate must have a written agreement with the busin6ess 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 for a covered entity that involve the use or disclosure of PHI on behalf of, or that provides services to, a covered entity.	A Covered California Certified Enrollment Counselor A third-party administrator that assists a health insurance company with claims processing A CPA firm whose accounting services involve access to PHI

When Can PHI be Used and Disclosed?

Permitted Uses and Disclosures

Consumers have an opportunity to agree or object to PHI use and disclosure. Informal permission may be obtained by asking the individual outright. 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

- To treatment, payment, and health care operation activities, such as doctor and hospital or health insurance company performance evaluations, audits, medical reviews, accreditation, business planning, de-identifying PHI, etc.
- 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 twelve 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
- In a 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

PHI should NEVER be sent via email. This includes screenshots from CoveredCA.com containing PHI.

Important

If you are unsure of the appropriate use of PHI, contact your direct supervisor before using or disclosing PHI. In your role working on behalf of Covered California, you will not have a direct need to access PHI. However, any PHI disclosed by consumers should be protected following the requirements described within this course.

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 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 for the results of a pre-employment physical or lab test
- Disclosures to a pharmaceutical firm for 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 or disclosures required by law

SAFEGUARDS AND THE PRIVACY RULE AND SECURITY RULE

The safeguard requirements of the Privacy Rule establish protections for all PHI regardless of form (paper, oral, or electronic). 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 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 are the technology, policy and procedures for its use that protect information system data and control access to it.

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.

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 OCR or with 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. Online at: http://www.hhs.gov/ocr/privacy/hipaa/complaints/hipcomplaintpackage.pdf
2. Consumers may submit a written complaint in their own format, which includes the following information:
    - Full name
    - Full address
    - Telephone numbers
    - Email 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

- Sign and date the complaint

The complaint can be mailed, emailed or faxed to the appropriate OCR regional office (based on where the alleged violation took place). The complaint must be filed within 180 days of the Privacy Rule or Security Rule violation. Locations and fax numbers can be found online at:

http://www.hhs.gov/ocr/office/about/rgn-hqaddresses.html or email: OCRComplaint@hhs.gov

4. What Is Federal Tax Information (FTI)?

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, claims for a 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.

What are the Special Privacy and Security Rules for FTI?

The IRS has very strict rules on who is permitted to see 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 annual recertification 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:

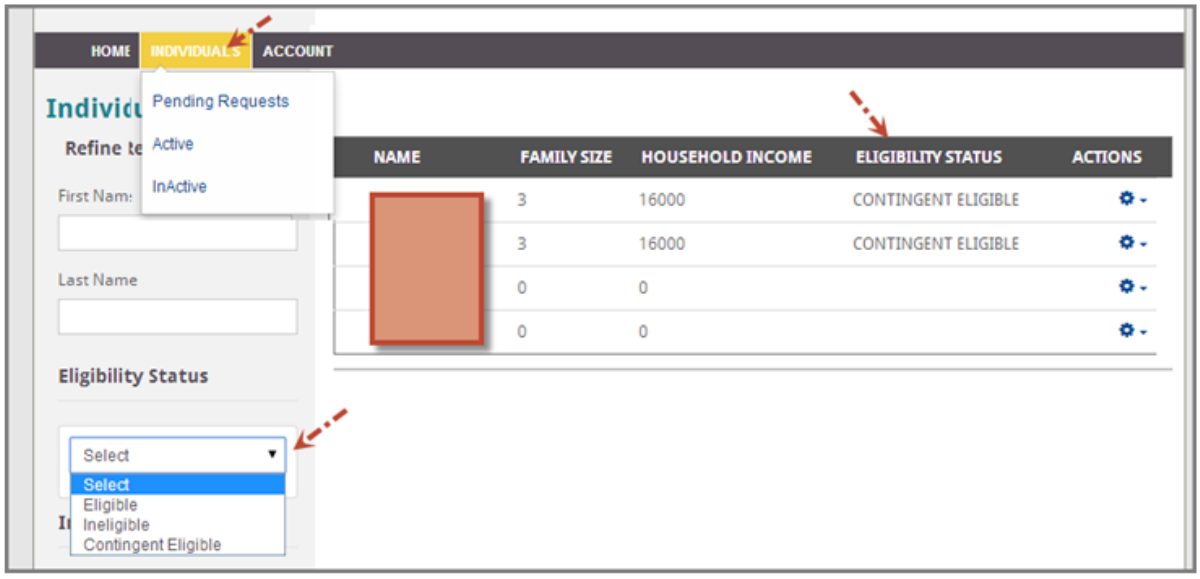
- FTI must never be left unattended
- FTI must be labeled as being "FTI" and must be tracked
- FTI must be protected with two physical barriers. For example, it must be placed inside a secured perimeter and in a locked container, or secured in a locked perimeter and secured interior, or in a locked perimeter and a secured 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 destruction bins
- Electronic and encrypted media must be destroyed using methods approved by Covered California's Information Security Officer. Those assisting consumers with enrollment should never have a need to use FTI outside of CoveredCA.com and the application process

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

Those assisting consumers on behalf of Covered California will be exposed to family size and household income FTI. If information identifying individuals is removed as the example above illustrates (i.e. name), it is not considered a prohibited disclosure. The example below illustrates a screen shot from the CEC dashboard on CoveredCA.com that hides the names of the consumers, thus avoiding a violation of prohibited disclosure of FTI:



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.

Reporting Violations or Suspected Violations of FTI

Covered California staff must follow the special rules and safeguards that apply to FTI. Remember, only staff with special authorization are permitted to have access to FTI and only if they have a business need. 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 Privacy Officer:

Phone: 1-800-889-3871
Email: PrivacyOfficer@covered.ca.gov

5. Penalties For Violations Of Compliance and Privacy Laws

Penalties Under the Affordable Care Act, 45, C.F.R. 155.260

Under the ACA, information provided by applicants may be used only for the purposes of, and to the extent necessary in, ensuring the efficient operation of Covered California, 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)). The following penalty applies to those who 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 CFR 155.260(g)).

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 $5,000 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 addition to general damages, a minimum of $25,000 may be imposed as punitive damages, plus attorney fees and costs (Calif. Civil Code, section 1798.53).

PENALTIES UNDER IRS RULES

FTI can be used only for an authorized purpose and only to the extent authorized. The penalties for unauthorized disclosures and access 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 imprisonment up to five years, or both (26 U.S.C. 7213)
- It is unlawful for any person to willfully 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)

HIPAA PENALTIES FOR COVERED ENTITIES AND BUSINESS ASSOCIATES

Under HIPAA, civil monetary 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 $1,000 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 ten years

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 offenses that are punishable by fine and imprisonment in county jail

Penalties and Laws

There are a number of laws in place to prevent fraud, waste and abuse. Each one addresses a specific issue or set of issues and has strict consequences that depend on the violation. The penalties can include:

- Civil monetary penalties (CMPs)
- Criminal conviction/fines
- Civil prosecution
- Imprisonment
- Loss of license (Certified Insurance Agents)

Good to Know
The use of the word civil here refers to the laws that govern the private rights of individuals and related legal proceedings. Civil law is different from criminal law.

- Exclusion from federal health care programs

For people working for or on behalf of Covered California, any incident of fraud, waste or abuse is grounds for immediate termination from program participation. As such, it is important to be familiar with the laws that are relevant to your work with Covered California and which are necessary in protecting against fraud, waste and abuse.

EMPLOYEE CONSEQUENCES

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).

6. REPORTING PRIVACY, SECURITY AND COMPLIANCE INCIDENTS

REPORTING CONCERNS AND INCIDENTS

Everyone who works for or on behalf of Covered California has the right and the responsibility to immediately report any actual or possible Code violations whether a result of personal conduct or that of another worker, supervisor, officer or director. No concern is too small or unimportant. If you have a concern or need guidance, seek one of the following resources:

- Talk to your supervisor who knows you and the details of your role with Covered California
- Talk to your organization's designated Covered California representative
- If you do not feel comfortable reporting your concerns to your supervisor or designated representative you may contact Covered California directly with specific information about the alleged concerns:

Covered California
1601 Exposition Blvd.
Sacramento, CA 95815
1-800-300-1506

Covered California is committed to ensuring that no one will ever suffer retaliation for seeking guidance or reporting ethical concerns or violations.

DUTY TO DETECT AND REPORT INCIDENTS

All Covered California staff, contractors and vendors who have access to Covered California data systems, services or networks, or access to any confidential information (PII, PHI, FTI) 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 action to prevent harm and will direct you on what action to take
- The duty to report includes both security and privacy incidents

SECURITY INCIDENTS

A security incident is defined as any real or potential attempt (successful or unsuccessful) to access or adversely affect, or both, Covered California data, systems, services or networks, including online 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**s – a person gains electronic 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 CoveredCA.com asset is lost or personal belongings of a Covered California employee or contractor are stolen at a work location

PRIVACY INCIDENTS

A Privacy Incident is defined as the attempted or successful unauthorized access, use, disclosure, modification or destruction of PII, PHI, FTI, or interference with operations of 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 Covered California employees contact information is posted on a public website and 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 and sends files with applicants' personal information to their 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

Reporting Privacy and Security Incidents

You must **IMMEDIATELY REPORT** a suspected or actual security or privacy incident to your supervisor and contact Covered California Information Security at:

Email: PrivacyOfficer@covered.ca.gov

Telephone: 1-800-889-3871

When an incident has been reported, an Information Security Officer 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.

Immediate Action in Reporting Incidents

Based upon the information received, 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 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 in keeping Covered California's confidential information and its data systems, services and networks safe and protected.

7. Increasing Information Security Awareness

Information Security Safeguards

The table below provide examples of administrative, technical and physical safeguards required as part of the Privacy Rule and Security Rule.

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	• Implement policies and procedures to limit physical access to electronic information systems, while ensuring that properly

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 a security awareness and training program for all members of the workforce. • Implement procedures for the authorization and supervision, or both, 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 to address security incidents. • Establish policies and procedures for responding to an emergency or other occurrence (e.g. fire or vandalism,) that can damages systems that contain sensitive data.	those persons that have been granted access rights. • Assign a unique name or number, or both, for identifying and tracking user identity. • Implement hardware, software and 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.	authorized access is allowed. • Implement policies and procedures to safeguard the facility and equipment 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 to restrict access to authorized users only. Keep laptop computers containing data 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 to address the final disposition of data.

KEEPING YOUR PASSWORDS SAFE

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

- The best passwords use a combination of numbers, upper and lowercase letters and special characters such as: * & $
- Passwords should be at least eight 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 for you to remember but hard for someone else to guess

Guidelines for keeping your passwords safe

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

Any suspected unauthorized use of your user ID or password must be reported immediately to your supervisor. Do not share your CoveredCA.com username name and password with anyone.

PROTECTING YOUR WORKSTATION, LAPTOP AND MOBILE DEVICE

Protecting your workstation

Securing information when you leave your computer or workstation is critical to maintaining information security. Below 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, such as smart phones, that have network access
- Ensure paper documents are secure at all times. Lock your desk 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

You are responsible for the confidentiality/security of your mobile devices. If your mobile device is lost or stolen and contains sensitive consumer information, you must report it to your supervisor and Covered California immediately. The table below shows ways to protect mobile devices and laptops.

Methods to Secure Mobile Devices/Laptop	
Mobile Device	**Laptop**
• Turn off Bluetooth discovery mode • Avoid public Wi-Fi hotspots • Beware of text message spam • Be selective with smart phone applications • Do not store passwords on your phone • Avoid check-ins, turn off geotagging • Download security updates and back-up your data regularly	• Always use a docking station or laptop security cable • Use a username and password to login to your laptop. Setup an automatic log off after a pre-determined period of inactivity • Data encryption • Virus protection • Symantec endpoint protection • Antivirus application

SECURITY WHILE TRAVELING AND WORKING REMOTELY

Below is a list of safeguards to help increase security while traveling and working remotely:

- Encrypt your data
- Carry your laptop with you, avoid setting your laptop/tablet on the floor
- 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
- Remove sensitive data from your portable computer to a thumb drive or other protect storage device

EMAIL SECURITY

When using email, slow down, think and check before hitting "send." Common mistakes include:

- Auto-complete: email systems complete addresses before you finish typing. Always verify the name and the email address before you hit "send".
- Copying and blind copying (cc/bcc): review 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 Don'ts of Email Security	
Do's	**Don'ts**
Open emails only from people you know and trust	Do not provide your email, or someone else's email, address online
Open only those email attachments whose headings or texts sound familiar	Do not trust a site just because it claims to be secure
Use email encryption for particularly sensitive messages.	Do not open email attachments containing the following file extensions: .exe, .bat, .reg, .scr, .dll, or .pif
Delete suspicious messages	Do not provide your credit card number or other sensitive information by email
Check out a website's business purpose and content before sending any sensitive information	Do not provide personal information by email, unless you are certain of a person or organization's authority to ask for it
	Do not open emails addressed to people other than you.
	Do not respond to emails that request your personal or financial information.

Sending Sensitive Information over Email

It is the policy of Covered California that a completed paper application must NEVER be sent via email. In fact, to protect yourself and consumers, any two pieces of information that identify a consumer (e.g. name and phone number) is considered PII and should never be sent in the body of an email message. If there is a business need to send PII over email, this information should be put into a document that can be encrypted then sent as an attachment to an email message.

How to Password Protect and Encrypt Documents

There are a number of ways to protect your files with a password in order to add another layer of security, especially when sending documents over email. Password protecting a file or document means that the file is being encrypted so it cannot be opened or understood without a password.

Steps to password protect in Microsoft Office:

1. Open the file or document you want to encrypt
2. Go to "File" in the menu bar
3. Select the "Info" tab
4. Select "Protect Document" (Word), "Protect Workbook" (Excel), "Protect Presentation" (PowerPoint)
5. Click "Encrypt with Password"

6. The dialog box will provide a display to enter a password (up to 25 characters)
7. Enter the password two times to confirm
8. Click “OK” then save the document

When the document is sent via email the password will be required to open and read the document. The password should be sent in an email separate from the document so that someone who intercepts the email does not have access to the document and password simultaneously. You cannot open the document without the password and the password is useless without access to the document.

PAYMENT CARD SECURITY

During the application process consumers are asked if they would like to pay the first month’s premium at that time or at a later date. If the consumer wishes to pay the premium at that time, the consumer must enter this information personally into CoveredCA.com. Those who assist consumers with enrollment are strictly prohibited from entering payment information on behalf of the consumer.

COMPUTER SECURITY: VIRUSES, MALWARE AND PHISHING

There are thousands of types of malicious software, also known as malware. Some examples include, viruses, worms, spyware, Trojan horses or rogue security software.

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

- Your computer runs more slower than normal
- Your computer stops responding or freezes often
- Your computer crashes and restarts every few minutes
- You see distorted menus and dialog boxes
- Disks or disk drives are inaccessible
- 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 or 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 emails typically contain a generic greeting and a warning of a sudden change in an account that requires entering private information to correct. These messages typically contain poor spelling or grammar.

Here are some ways to avoid phishing scams:

- Question impersonal emails
- Be wary of requests for confidential information

- Question the scare tactic message
- Do not reply to any email 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

Social Media Safety

Social media sources are services people use to connect with others to share information and promote products or services, or both. Some of the most common examples include: Facebook, Twitter, Instagram, and 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 identity secure. Tips for social media protection include:

- Create a social specific email
- Do not use your Covered California email 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
- Remember that downloading videos increases susceptibility to viruses

Social engineering is the art of manipulating people so they give up confidential information. Attackers use email, 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 email messages
- Do not reveal personal or financial information in emails or follow links sent in suspicious emails
- 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

8. What is Compliance?

Compliance is a very important part of Covered California. To be in compliance, you are required to act in accordance with all of the applicable laws and regulations as well as your agreement with Covered California. This includes the Affordable Care Act, regulations by the US Department of Health and Human Services, California State law and regulations specific to Covered California. In addition, this includes following Covered California's specific guidelines

for maintaining privacy and security, avoiding conflicts of interest and helping to prevent fraud, waste and abuse.

It is vitally important that everyone who works with consumers in their role with Covered California knows and follows the compliance standards, expectations and responsibilities that govern all Covered California work.

Compliance, or being compliant, means following guidelines for:

- Maintaining privacy and security
- Avoiding conflicts of interest
- Helping to prevent fraud, waste and abuse

TAKING PERSONAL RESPONSIBILITY

If you work with consumers in your role with Covered California, you are responsible for professional conduct. This means you should always:

- Listen attentively so you can provide consumers with the best service to meet their needs.
- Possess the knowledge and expertise needed to provide Californians with clear, accurate information about their health coverage options.
- Work to understand the culture, background and needs of the people served.
- Provide fair, impartial and accurate information to consumers in a professional manner with courtesy, patience and understanding.
- Make sure consumers have equal access to information without discrimination to age, gender, disability, race, creed, national origin or economic background.
- Earn consumer trust by demonstrating accountability, responsiveness, reliability and cooperation.

MAKING ETHICAL DECISIONS

The success of Covered California also depends on ethical decision-making. We make many decisions every day and most do not raise ethical questions. Those that do are decisions that could hurt a consumer, group of people or the reputation and mission of Covered California. Choices between alternatives that might be good or bad, depending on your perspective, are ethical decisions. So are choices between two good or two potentially bad alternatives.

Good to Know

Ask yourself these three questions to guide ethical decision-making:

1. Is the action or decision against the law? Does it appear to violate a law or regulation?
2. Does the action or decision go against the vision, mission or values of Covered California?
3. If my action or decision made the front page of a newspaper, would I be proud or horrified?
4. If your answer is YES to any one of these questions, do not take the action or make the decision.

COMPLYING WITH THE LAW

Health insurance is one of the most regulated industries in the US. Full compliance with all applicable laws, regulations and contractual obligations is unconditionally required. Entities receiving funding from Covered California must reference their contract to ensure they are complying with the law.

You should make every effort to understand and follow the laws, regulations and compliance processes that apply to your role. This includes helping colleagues and others ensure that basic processes are compliant.

Compliance is not optional. If an action or decision is noncompliant, it is strictly prohibited.

If there is ever a time when you are not sure whether a course of action is legal or ethical, talk with your supervisor. You may also contact a Covered California designated representative.

WORKING WITH CONSUMERS AND PEERS

All consumers interacting with Covered California have the right to be treated with courtesy and respect. One of the ways to accomplish this is to be sensitive and attentive to the many populations that make up California. These include:

- Communities of color
- Low-income families
- Individuals who have limited English proficiency or who are not functionally literate
- Families of individuals with special health care needs
- Individuals with physical or mental disabilities
- Individuals with substance abuse issues
- Individuals of different cultures and backgrounds

Supporting the diversity of Californians includes developing and maintaining general knowledge about the racial, ethnic, and cultural groups in your service area, including each group's diverse cultural health beliefs and practices, preferred languages, health literacy, and other needs.

Exhibiting professionalism, and treating others with courtesy and respect, should extend to all those that you interact with on behalf of Covered California, including your peers.

HONESTY AND FAIRNESS

To ensure honesty and fairness in the education and application process for Covered California, insurance plan options must always be represented fairly and equitably. Only provide recommendations regarding specific plans, doctors or hospitals over another where permitted for the role (e.g. Certified Insurance Agents or Plan-Based Enrollers). Consumers must be provided with information about the full range of Covered California health plan and Medi-Cal options, and financial assistance programs for which they are eligible.

PROTECTING CONFIDENTIALITY

Consumer confidentiality is a key priority of Covered California. Protecting confidentiality applies to all applicants and within all areas of Covered California.

Disclosure of information that identifies name, address or Social Security Number of any Covered California applicant, without the consent of the applicant, is prohibited and punishable

by law. Disclosure of personal information may result in civil monetary penalties. Breach of confidentiality is grounds for immediate termination of your role with Covered California.

Everyone who works for or on behalf of Covered California, especially if you work directly with consumers, must follow these basic confidentiality guidelines:

- Safeguard ALL information about applicants and their families, including their name, address, Social Security Number, health status and income.
- Handle consumer financial and tax information with the highest level of security and privacy.
- Keep your speaking voice low when discussing personal information with a consumer.
- Do not talk about applicants with coworkers or other applicants.
- Ensure that applicants do not receive solicitations or get placed on any mailing lists as a result of their contact with Covered California.
- Protect all financial, statistical, personal, technical and other data and information related to Covered California's operations that is not publicly available.

Everyone who works for or on behalf of Covered California is required to protect applicant privacy and ensure all personal information is kept secure. This means that you:

1. Are responsible for keeping all consumer information private and confidential. Consumer information includes name, address, Social Security number, financial records and health status.
    - Use and discuss applicant information only when necessary for your role with Covered California
    - Do not share information with unauthorized persons
    - Use applicant personal and health information only for the reasons it was intended, or as the applicant allows, or the law requires
    - Do not disclose confidential information that violates the privacy rights of consumers
    - Do not request, store or disclose a consumer's CoveredCA.com username and password
2. Handle all applicant information and materials, including paper applications and records, electronic records, faxes and mail, in a way that protects confidentiality and privacy.
3. Maintain security by:
    - Ensuring that electronic correspondence with confidential information is NOT sent over the Internet unless encrypted or on a secure network
    - Only storing private or confidential information on portable electronic devices or media if they are encrypted within acceptable standards
    - Maintaining secure methods for exchanging personal information
    - Shredding and properly disposing of paper documents
    - Promptly deleting uploaded private or confidential information from electronic devices, after the information has been processed

Protecting consumer information is so important that the Code of Federal Regulations (45 CFR § 155.260) imposes a civil penalty of up to $25,000 for knowingly and willfully using or disclosing consumer health or financial information. The penalty is per person or entity, per use or disclosure, in addition to other penalties that may be prescribed by law.

This is just a brief introduction to the topic of privacy. The Privacy and Security course goes into depth on this topic.

9. Conflict of Interest

What is a Conflict of Interest?

A conflict of interest is when someone has personal or private interests that may conflict with the organization or company that has hired them to do a job. For Covered California, a conflict of interest means having a private or personal interest that could influence or appear to influence your official Covered California duties.

A conflict of interest is a situation, not an action. It can be real or perceived. Either way, conflicts of interest can harm Covered California's purpose and reputation by:

- Lowering consumer trust
- Creating roadblocks in persuading the uninsured to get coverage
- Making Covered California seem unreliable

Avoiding a conflict of interest starts by knowing how to identify one. Following are a few examples of situations that could be a conflict of interest with Covered California:

- A Covered California service provider takes on other responsibilities that make it difficult to perform their role objectively and effectively
- A Covered California service provider owns stock in a California health insurance company that is also a Covered California health plan
- A Covered California service provider, not authorized to do so in the normal course of their duties, recommends one health insurance company, doctor or hospital over others to consumers because they are receiving payment or some other benefit for making the recommendation.
- A Covered California service provider accepts a gift from a health insurance company for recommending the plan to consumers
- A Covered California service provider accepts free exhibit space at an event sponsored by a health insurance company

Having a conflict of interest does not equal corruption or unlawful behavior unless the person who has the conflict does nothing about it.

Avoiding Conflicts of Interest

Covered California has specific guidelines for avoiding two common situations that can create a conflict of interest: disclosure and gifts and entertainment.

Disclosure

To avoid conflicts of interest, you are required to provide to all consumers with whom you interact, a clear and concise description of the services you will perform for them and disclosure of how you will be paid for those services. Consumers should also be told that they may select or change Covered California service providers at any time.

Gifts and Entertainment

Gifts, favors or improper incentives of any kind can create the appearance of a conflict of interest. People who work for or on behalf of Covered California may never accept gifts of money or solicit nonmonetary gifts from organizations that do business with Covered California (or that may enter into a financial arrangement with Covered California).

It is also not acceptable for anyone who works for or on behalf of Covered California to offer gifts to consumers or others in the course of their work with Covered California.

Disclosing Conflicts of Interest

Everyone working for or on behalf of Covered California is required to disclose situations that could be considered a conflict of interest. If you find yourself with a real or potential conflict of interest, you must immediately:

- Disclose the conflict to Covered California by notifying your supervisor
- Take action immediately to eliminate the conflict or withdraw from your role with Covered California

If you are not sure if you have a conflict of interest or if you need help avoiding one, there are several resources available:

- Talk to your supervisor
- If you feel more comfortable, you can contact your Covered California designated representative

Anyone working for or on behalf of Covered California who has a conflict of interest and does not disclose it will be subject to disciplinary action up to and including termination of their role with Covered California.

10. Fraud, Waste and Abuse

Millions of dollars are improperly spent every year because of fraud, waste and abuse. It affects our state, our communities and each of us. Everyone working for or on behalf of Covered California plays a vital role in the effort to prevent, detect and report possible fraud, waste and abuse. This section details what defines fraud, waste and abuse, the differences among them, penalties and reporting.

Definitions of and Differences Between Fraud, Waste and Abuse

The Centers for Medicare and Medicaid Services (CMS) is a branch of the US Department of Health and Human Services. CMS is the federal agency that administers Medicare, Medicaid and the Targeted Low-Income Children's Program and provides information for health professionals, regional governments and consumers.

As part of its role, CMS has developed extensive policies and guidelines about fraud, waste and abuse. Many of the definitions described in this section come from CMS.

Fraud

Fraud is the intentional submission of false information to get money or a benefit. Fraud may be committed against the government, an organization or an individual. Fraud occurs when an individual knows or should know that something is false and provides information or conceals material facts with the intent to deceive to benefit themselves or another person.

Examples of Fraud

- Falsifying information on an enrollment application for a consumer
- Submitting an enrollment application for an individual that does not exist
- Soliciting, offering or receiving a kickback, bribe or rebate
- Forging or altering required documentation on an enrollment application
- Deliberately misrepresenting the services offered by Covered California, resulting in unnecessary cost, improper payments or overpayment
- Using someone else's coverage or insurance card

Waste

Waste is the extravagant, careless or needless expenditure of government resources or services that result from deficient practices or decisions. An example of waste would be throwing away collateral and marketing materials provided by Covered California and intended for the public.

Abuse

Abuse describes practices that either directly or indirectly results in unnecessary costs. Unlike fraud, there is no intention to deceive.

Examples of Abuse

- Breaking public trust by charging a fee for application assistance
- Providing and charging for other services that are not necessary for enrollment such as notarizing an enrollment application

Differences between Fraud, Waste and Abuse

One of the primary differences between fraud, waste and abuse is intent and knowledge. Fraud requires:

- The intent to obtain payment or a benefit; and
- The knowledge that the action is wrong.

Neither waste nor abuse requires intent and knowledge.

If there is a situation that concerns you, you should report it directly to Covered California's Consumer Protection Unit:

Covered California
Office of Consumer Protection
1601 Exposition Blvd
Sacramento, CA 95815
1-800-300-1506
Consumerprotection@covered.ca.gov

Recognizing Red Flags

It is important to be on the lookout for suspicious activity that might be fraud, waste or abuse in order to protect Covered California from potential abuse practices, civil liability and perhaps criminal activity. Among the things to stay alert for are:

- Websites that represent themselves as Covered California
- Individuals who represent themselves as working on behalf of Covered California and are charging for their services (i.e., a fee for application assistance)
- Individuals who are at a public event and are not performing their duties (i.e., not engaging with the public or speaking disrespectfully to the public)
- Misuse, destruction or vandalism of Covered California property, such as collateral material, displays or electronic devices

False Claims Act

The Federal False Claims Act (32 USC 3729) and California Government Code 12650 prohibits knowingly and willfully executing, or attempting to execute, a scheme or deception:

- To defraud any health care benefit program
- To obtain (by means of false and fraudulent pretenses, representations or promises) any of the money or property owned by or under the custody or control of, any health benefit program in connection with the delivery of or payment for health care benefits, items or services

Good to Know
The False Claims Act language is complex. It is included here for your reference.

Proof of actual knowledge of the law or specific intent to violate the law is **not** required. Penalties for violating the False Claims Act may include fines, imprisonment or both.

Reporting Fraud, Waste or Abuse

If you uncover or suspect potential fraud, waste or abuse, you are required to report it immediately to your supervisor. You may also report fraud, waste and abuse concerns at the Covered California, state or federal level.

You may choose to remain anonymous and complaint information entered in the record systems will not be traceable to you. In many cases, however, the lack of contact information for the source prevents a comprehensive review of the complaint. You are encouraged to provide information on how to contact you for additional information.

11. ACTIVITIES

Activity 1

Fill in the blanks

1. Entities must follow the Privacy and Security Rules are called _____ entities.
2. Information that is used in the 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. A central aspect of the Privacy Rule is the principle of _____ _____use and disclosure.
5. 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.
6. When a covered entity can use and disclose an individual's PHI it is called _____ use and disclosure.
7. Open only those email attachments whose headings or text sound _____.
8. When using email, slow down, _____, and check before hitting send.
9. Do not send _____ information over the internet before checking the website security.
10. Do not open attachments to emails from _____ sources.
11. Your computer may be infected with a virus if it runs more _____.
12. To protect against computer viruses, do not _____on attachment files whose names end with .nws.
13. Some rogue security software might install _____to steal your data.
14. Any communication that begins with "Dear Bank of America Customer:" should signal _____.

Activity 2

Test your knowledge		
	True	**False**
1. The compliance requirements only apply to employees of Covered California.		
2. It is unethical to make decisions that could hurt a consumer, group of people or are inconsistent with the mission of Covered California.		
3. You have the right and responsibility to report violations and ethical concerns.		
4. Earning consumer trust is one way of taking personal responsibility as a representative of Covered California.		
5. It is okay to mail a paper application for a consumer.		
6. Sharing an applicant's Social Security Number is okay in some situations.		
7. PII stands for personally identifiable information		
8. Someone's driver's license is not PII		
9. One way to protect PII is to use the full Social Security number of an individual		
10. FTI stands for federal tax information		
11. A secure password should be five alphabet letters or less.		
12. You should write down your passwords so you do not forget them.		
13. When you leave your workstation, you should log off or lock your workstation.		
14. Store your passwords on your smart phone so you do not forget them.		
15. If you see a good software program, install it on your laptop.		
16. Do not put your name or contact information on a laptop/tablet.		
17. Disable file and printer sharing so that you are less vulnerable to hackers.		

Test your knowledge		
18. If you leave your laptop/tablet in your hotel room, use a security cable to secure the laptop.		
19. If you receive an unsolicited phone call, asking for information about Covered California, such as networks, you should reveal this information.		
20. If an email message conveys a sense of urgency, you should act quickly.		
21. The most prevalent type of social engineering attack is conducted by phone.		
22. A common social engineering tactic is impersonation on help desk calls.		

12. ACTIVITY ANSWERS

Activity 1

1. Covered
2. Protected Health Information
3. Two
4. Minimum & Necessary
5. Written authorization
6. Permitted
7. Familiar
8. Think
9. Sensitive
10. Unfamiliar
11. Slowly
12. Click
13. Malware
14. Phishing

Activity 2

1. False
2. True
3. True
4. True
5. False
6. False
7. True
8. False
9. False
10. True
11. False
12. False
13. True
14. False
15. False
16. False
17. True
18. True
19. False
20. False
21. True
22. True

13. ENDNOTES

[1] Source: 45 CFR §164.308

[2] Source: 45 CFR §164.312

[3] Source: 45 CFR §164.310