Privacy and Information Security for Enrollers Quick Guide

Background

This Quick Guide will help Enrollers understand categories of sensitive and confidential information that need to be protected under the law. This guide will help cover penalties for failing to protect sensitive and confidential information and important steps to take to prevent those.

Personally Identifiable Information

Personally Identifiable Information (PII), is any information that identifies or describes an individual either by itself or when combined with other information.

Some examples of PII include:

- Full name
- Birthplace
- Email address
- Social Security Number (SSN)
- Covered California account or case numbers

Federal Principles

The Affordable Care Act Regulations governing privacy and security require Covered California to establish and implement privacy and security-related standards based upon 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 creation, 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 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 nonadherence and breaches.

Consumer Privacy Rights

- To inspect and obtain a copy of records containing their personal information
- To request correction of any records containing their personal information
- To request a preferred method of confidential communications
- 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 following the instruction provided by Covered California within the Privacy Policy page of the Covered California website at www.coveredca.com/privacy.

Covered California privacy standards also require those who are provided access to consumer PII to only collect or disclose the PII which is **strictly necessary** to determine eligibility for health coverage.

For example, if a member of the family is not applying for coverage, that person is not required to provide their social security number or immigration status. Only those who are applying for coverage need to provide that information.

Consent to Share

In order to disclose or use PII, Covered California and its contractors must either have permission from the individual or disclose the PII strictly for the purposes for which the individual provided it.

During the application and enrollment process, you may be asked to upload personal information on behalf of the consumer. You should explain to the consumer that you will only use the information to determine eligibility for, and help them enroll in, affordable health insurance coverage.

Unless you have consent from the consumer, the consumer's PII should never be retained or stored by you or your office. Copies, whether physical or electronic, must be deleted, destroyed or returned to the consumer when you no longer need it to perform the activity for which the consumer gave it to you.

Violations

Covered California privacy and security standards are designed to prevent the unauthorized disclosure or use of consumer PII and to protect the integrity of any such consumer PII by preventing unauthorized users from modifying or destroying it without the consumer's consent.

Third-party contractors, such as navigators and agents, who acquire access to consumer PII through the healthcare marketplace are required by contract to abide by Covered California privacy and security standards and policies. Those who fail to abide by any such standards or policies may be subject to contract termination.

Compliance with applicable privacy and security-related laws pertaining to consumer PII is required of all contractors who participate in the healthcare marketplace.

In addition to potential contract termination, contractors that violate any such privacy or security-related laws may also be subject to potential criminal or civil penalties depending upon the severity of the violation.

Criminal and civil penalties may include:

- Criminal conviction
- Civil prosecution
- Imprisonment
- Monetary fines

As such, it is important to be familiar with the laws that are relevant to your work with Covered California that are necessary to protect consumer PII.

Safeguards and Protection

Administrative:

- Implement policies and procedures to prevent, detect, contain, and correct security violations.
- Conduct an accurate and thorough assessment of the 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 damage systems that contain sensitive data.

Example: implement a security awareness and training program for all members on the workforce.

Technical:

- Implement technical policies and procedures for electronic information systems that maintain data to allow access only to 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.

Example: implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

Physical:

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

Example: implement procedures to control and validate a person's access to a facility based on their role or function, including visitor control, and control of access to software programs for testing and revision.

Strong Passwords

Tips for creating strong passwords:

- Make long passwords; 15 characters is a good minimum length.
- Do not use the word "password."
- Avoid using single words found in a dictionary.
- Don't use personal information like your birthday or name in your password.
- Avoid using memorable keyboard paths for your password, such as "qwerty."
- Pass-phrases or sentences (with special characters). Here are some examples but don't use these:
- Enjoy reading? Try "1L0ve2r3adb00ks!" spelled this way.
- Is the traffic bad on 50 today? Try "TrfcBd0n502day!"
- You can also combine nouns, characters, foreign vocabulary, month, etc.

Workspace Protection

Securing information when you leave your computer or workstation is critical to maintaining information security.

Some practices that will help safeguard information while stepping away from your desk include the following:

- Lock or log off from your desktop, laptop and/or smart phones when away for any period of time.
- Organize your workspace so that the workstation screen is not visible to the public or household members.
- Ensure paper documents are secure at all times – don't leave documents containing sensitive data lying out in the open and lock them in a secure cabinet when not in use.

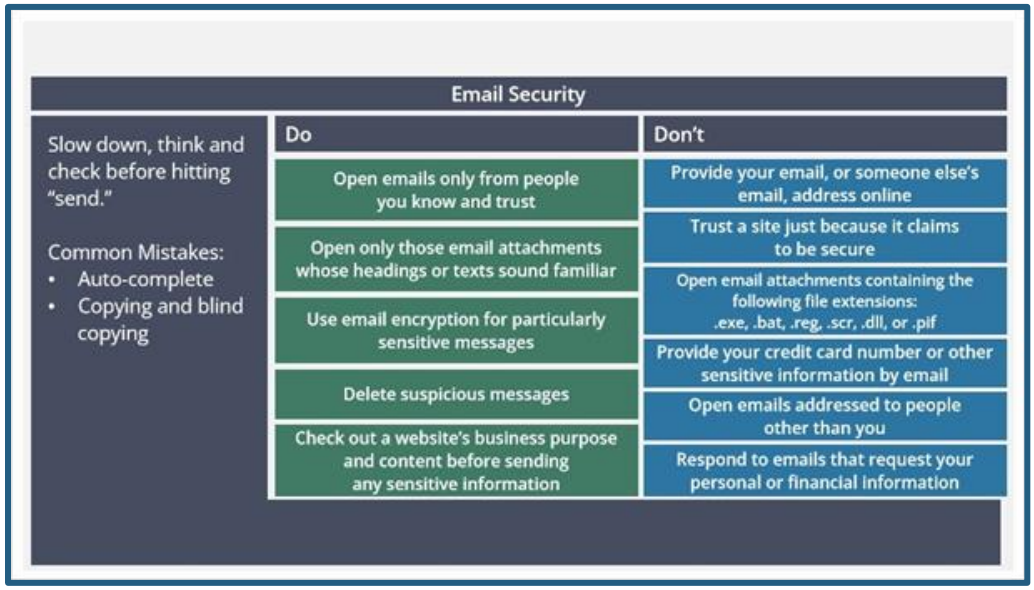
- Use only computers, networks, applications, and information for which you are authorized.

Email Security

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

- Autocomplete: email systems often complete addresses before you finish typing. Always verify the name and the email address before you hit "send".
- Copying and blind copying: be sure to 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.

Please review this chart for more do's and don'ts about email security.



Sensitive Information Through 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, PII should never be sent in the subject line or 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.

Protecting Files

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

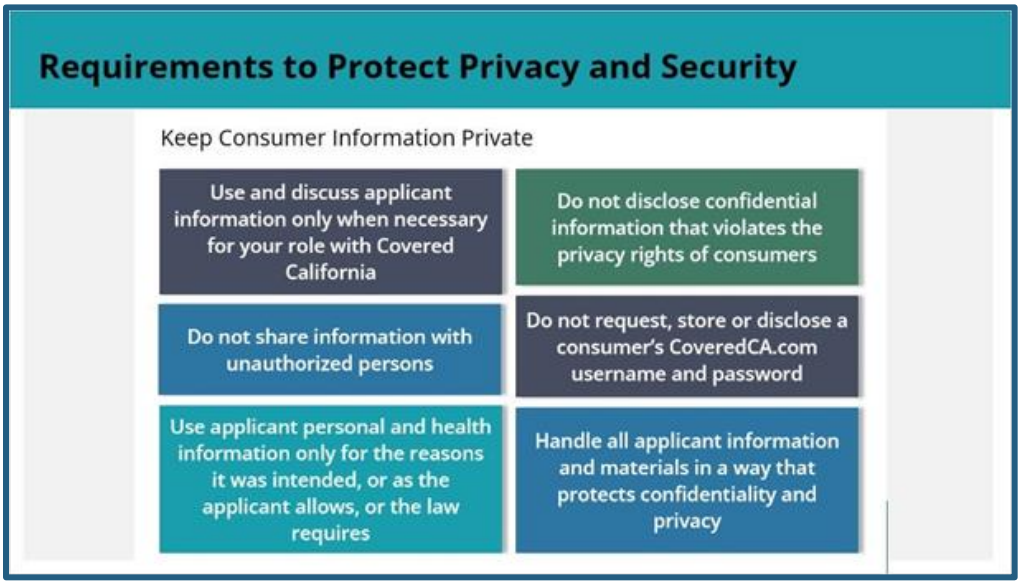
document means that the file is being encrypted so it cannot be opened or understood without a password.

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

Covered California Requirements

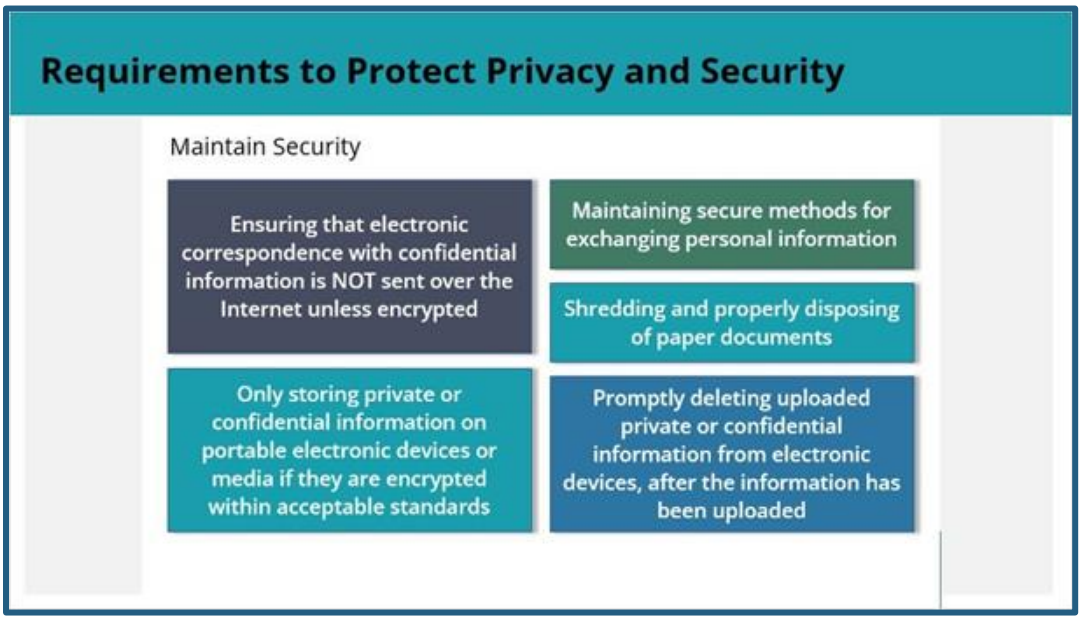
Everyone who works for or on behalf of Covered California is required to protect applicant privacy and ensure all personal information is kept secure. You are responsible for keeping all consumer information private and confidential. Consumer information includes, but is not limited to, name, address, Social Security number, financial records, and health status.



The guidelines required in your role to keep consumer information private include, but are not limited to the following:

- 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.
- Handle all applicant information and materials, including paper applications and records, electronic records, faxes and mail, in a way that protects confidentiality and privacy.



In your role with Covered California you must maintain security by:

- Ensuring that electronic correspondence with confidential information is NOT sent over the Internet unless encrypted.
- 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 uploaded.

Reporting Security and Privacy Incidents

Incident Reporting

Everyone who works for or on behalf of Covered California has the right and the responsibility to immediately report any actual or possible security or privacy incidents whether they are the result of personal conduct or that of another worker, supervisor, officer or director.

No incident is too small or unimportant.

Security Incidents	Privacy Incidents
A security incident is one that threatens the confidentiality, integrity, or availability of sensitive information. Examples: • Unauthorized electronic or physical access without permission to a network, system, application, or data • Malicious Code (virus, worm, Trojan horse, or other code-based malicious entity) that successfully infects a host • Denial of Service attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources	A privacy incident is one in which an unauthorized person and for an unauthorized purpose has access or potential access to consumer PII in usable form. Examples: • Misdirected fax or e-mails containing PII • Unauthorized disclosure of documents containing PII • Paper-based documents containing PII sent to wrong address • Consumer PII accidentally posted to publicly available website • Documents containing PII accidentally left in exposed area where they could be viewed by unauthorized person • Consumer PII accidentally added to the wrong application or account

A security incident is one that threatens the confidentiality, integrity, or availability of sensitive information.

Examples include:

- Unauthorized electronic or physical access without permission to a network, system, application, or data
- Malicious Code (virus, worm, Trojan horse, or other code-based malicious entity) that successfully infects a host
- Denial of Service attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources

A privacy incident is one in which an unauthorized person and for an unauthorized purpose has access or potential access to consumer PII in usable form.

Examples include:

- Misdirected fax or e-mails containing PII
- Unauthorized disclosure of documents containing PII
- Paper-based documents containing PII sent to wrong address

- Consumer PII accidentally posted to publicly available website
- Documents containing PII accidentally left in exposed area where they could be viewed by unauthorized person
- Consumer PII accidentally added to the wrong application or account

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 and Privacy Office staff will then take immediate action to prevent harm and will direct you on what action to take.
- This duty to report includes both privacy and security incidents.
- Failure to report a privacy or security incident may result in contract termination

You must IMMEDIATELY REPORT a suspected or actual security or privacy incident and contact the Covered California Information Security or Privacy Office through email at

InformationSecurity@covered.ca.gov

OR

PrivacyOfficer@covered.ca.gov

When you report an incident, an Information Security and Privacy Office staff member will send you an Incident Report Form to fill out with basic information about the incident, then will direct you on next steps.