

Sales Certification Series

Study Guide



2019-20



Agent Annual Training

Contents

2019-20 Agent Annual Training.....	3
1. Introduction.....	3
1.1 Privacy and Security Awareness.....	3
1.2 Background.....	4
1.3 Objectives.....	4
2. Personally Identifiable Information	5
2.1 Personally Identifiable Information.....	5
2.2 What is PII?	6
2.3 Covered CA Policy.....	7
2.4 Principles	7
2.5 Consumer Privacy Rights	9
2.6 Strictly Necessary	10
2.7 Consent to Share	11
2.8 Violations of Covered California Privacy and Security Standards	12
2.9 Violations of Privacy-Related Laws.....	13
3. Safeguards and Protection	14
3.1 Safeguards and Protection	14
3.2 Information Security Safeguards.....	14
3.3 Strong Passwords	16
3.4 Workstation Protection	17
3.5 Device and Laptop Protection	18
3.6 Travel and Remote Work.....	18
3.7 Email Security	19

3.8 Sensitive Info through Email.....	20
3.9 Protecting files.....	20
3.10 Social Media Safety	22
3.11 Covered CA Requirements	23
4. Reporting Security and Privacy Incidents	25
4.1 Reporting Security and Privacy Incidents	25
4.2 Reporting Security and Privacy Incidents	25
4.3 Your Duty to Report.....	26
4.4 Security Incidents	27
4.5 Immediately Report.....	28
4.6 California State Law	29
5. Voter Registration	30
5.1 Mandatory Voter Registration Assistance.....	30
5.2 Voter Registration Assistance.....	30
5.3 Voter Registration Assistance.....	31
5.4 Voter Registration Assistance – online application.....	32
5.5 Voter Registration Assistance – online application.....	33
5.6 Voter Registration Assistance – Online Application	33
5.7 Voter Registration Assistance – Paper Application	34
5.8 Voter Registration Assistance – Phone Assistance.....	35
5.9 Voter Registration Assistance.....	36
5.12 Options	37
6. Conclusion	38
6.1 Conclusion	38
6.2 Thank you	38

2019-20 Agent Annual Training

1. Introduction

1.1 Privacy and Security Awareness



Narration:

Welcome to the training course Privacy and Security Awareness.
This course will last approximately 40 minutes.

1.2 Background

Background

There are categories of sensitive, confidential information that need to be protected under the law. Protecting consumer information is a critical component of your role working on behalf of Covered California.

There are penalties for failure to protect confidentiality. In this course, we will cover those, as well as important steps you'll need to take to keep sensitive information safe.



Narration:

There are categories of sensitive, confidential information that need to be protected under the law. Protecting consumer information is a critical component of your role working on behalf of Covered California.

There are penalties for failure to protect confidentiality. In this course, we will cover those, as well as important steps you'll need to take to keep sensitive information safe.

1.3 Objectives



Objectives

- Define Personally Identifiable Information (PII) and understand its appropriate use.
- Identify applicable Covered California policies and procedures.
- Know how to protect confidential information.
- Understand Privacy and Security incidents and how to report them.

Narration:

In this course we will go over the following topics:

- Define Personally Identifiable Information (PII) and understand its appropriate use.
- Identify applicable Covered California policies and procedures
- Know how to protect confidential information
- Understand Privacy and Security incidents and how to report them.

2. Personably Identifiable Information

2.1 Personally Identifiable Information

**Narration:**

Personally Identifiable Information (PII)

2.2 What is PII?

What is Personally Identifiable Information (PII)?

Any information that identifies or describes an individual either by itself or when combined with other information.

Common Examples of PII	
Full Name	Birthplace
Email Address	Vehicle License Number
Credit Card Numbers	Country, State, Zip Code, City of Residence
Name of School Attended	Workplace
Live Scan 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 CA Account or Case Numbers

Narration:

Personally Identifiable Information, or PII, is any information that identifies or describes an individual


either by itself or when combined with other information.

Some examples of information that may be considered PII include:

- Full name
- Birthplace
- Email address
- Social Security Number,
- Covered California account numbers or case numbers

2.3 Covered CA Policy

Covered CA Policy



IMPORTANT TO REMEMBER:

The privacy and security laws and standards described in this training apply to Covered California state employees and everyone working on behalf of Covered California, including contractors.

Those who do not follow these laws and standards may be subject to the same fines, penalties and criminal punishment as personnel employed by the state.

Narration:

The privacy and security laws and standards described in this training apply to Covered California state employees and everyone working on behalf of Covered California, including contractors.

Those who do not follow these laws and standards may be subject to the same fines, penalties and criminal punishment as personnel employed by the state.

2.4 Principles

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.

Narration:

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

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 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

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

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:

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

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.

2.5 Consumer Privacy Rights

An Individual's Rights

Covered California has developed and implemented privacy-related standards based upon these principles to ensure that consumers have the following rights with regard to their PII:

- | | | |
|---|--|---|
|  To inspect and obtain a copy of records containing their personal information |  To request correction of any records containing 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 following the instructions provided by Covered California within the Privacy Policy page of its website located at www.coveredca.com/privacy.

Narration:

Covered California has developed and implemented privacy-related standards based upon these principles to ensure that consumers have the following rights with regard to their PII:

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

2.6 Strictly Necessary

Strictly Necessary

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.

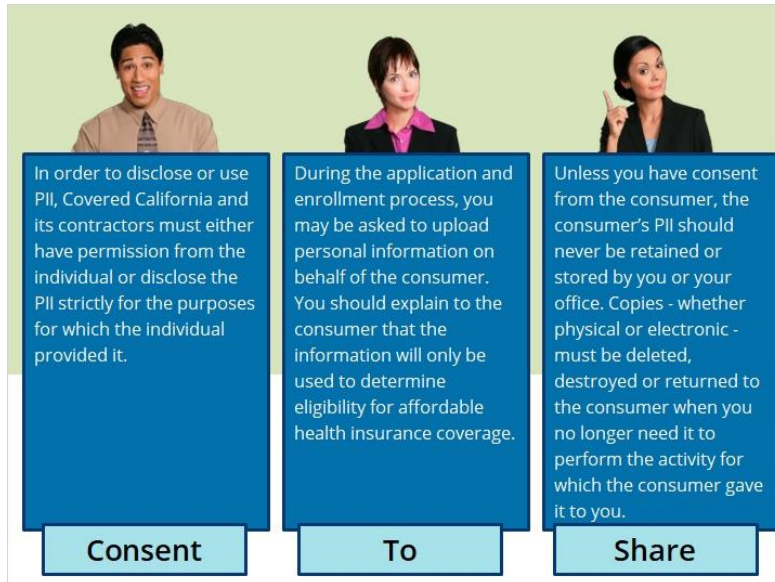
**Narration:**

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.

2.7 Consent to Share



<p>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.</p>	<p>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 the information will only be used to determine eligibility for affordable health insurance coverage.</p>	<p>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.</p>
Consent	To	Share

Narration:

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 the information will only be used to determine eligibility for affordable health insurance coverage.

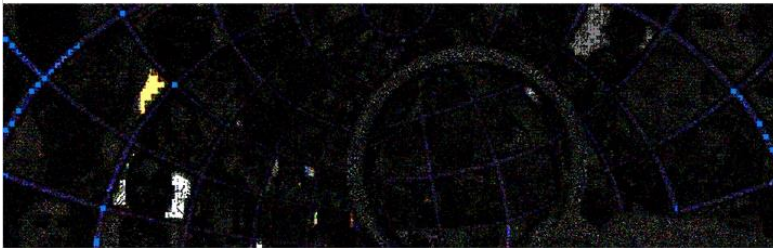
Unless you have consent from the consumer, the consumer's PII should never be retained or stored by you or your office. Copies - whether physical or electronic - must be deleted, destroyed or returned to the consumer when you no longer need it to perform the activity for which the consumer gave it to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

2.8 Violations of Covered California Privacy and Security Standards

Violations of Covered California Privacy and Security Standards

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 Exchange 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.



Narration:

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 Exchange 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.

2.9 Violations of Privacy-Related Laws

Violations of Privacy-Related Laws

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

In addition to potential contract termination, contractors which 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.



Narration:

Compliance with applicable privacy and security-related laws pertaining to consumer PII is required of all contractors who participate in the Exchange. In addition to potential contract termination, contractors which 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.

3. Safeguards and Protection

3.1 Safeguards and Protection



Narration:

Safeguards and Protection

3.2 Information Security Safeguards

Information Security Safeguards		
Examples of Required Security Rule Safeguards – Click to Enlarge		
ADMINISTRATIVE	TECHNICAL	PHYSICAL
<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> 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.

Narration:

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

Information Security Safeguards
Examples of Required Security Rule Safeguards – Click to Enlarge
ADMINISTRATIVE
<ul style="list-style-type: none"> • 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 damages systems that contain sensitive data.

An example of an administrative safeguard: implement a security awareness and training program for all members on the workforce.

Information Security Safeguards
Examples of Required Security Rule Safeguards – Click to Enlarge
TECHNICAL
<ul style="list-style-type: none"> • 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.

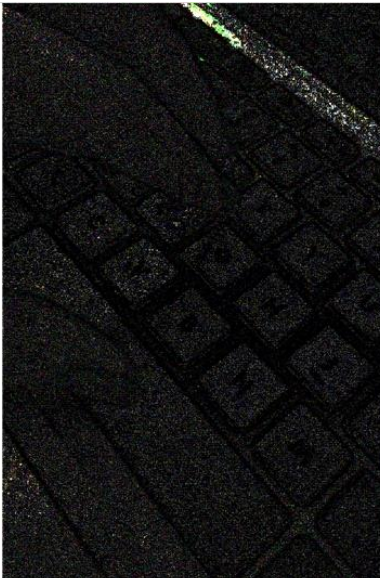
An example of a technical safeguard: implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

Information Security Safeguards
Examples of Required Security Rule Safeguards – Click to Enlarge
PHYSICAL
<ul style="list-style-type: none"> • 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.

An example of a physical safeguard: 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.

Click on each panel to enlarge the table.

3.3 Strong Passwords

<p>Creating Strong Passwords</p> <p>A good password is easy for you to remember but hard for someone else to guess.</p> <ul style="list-style-type: none"> • The best passwords use a combination of numbers, upper and lowercase letters and special 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 • Do not use dictionary words 	
--	--

Narration:

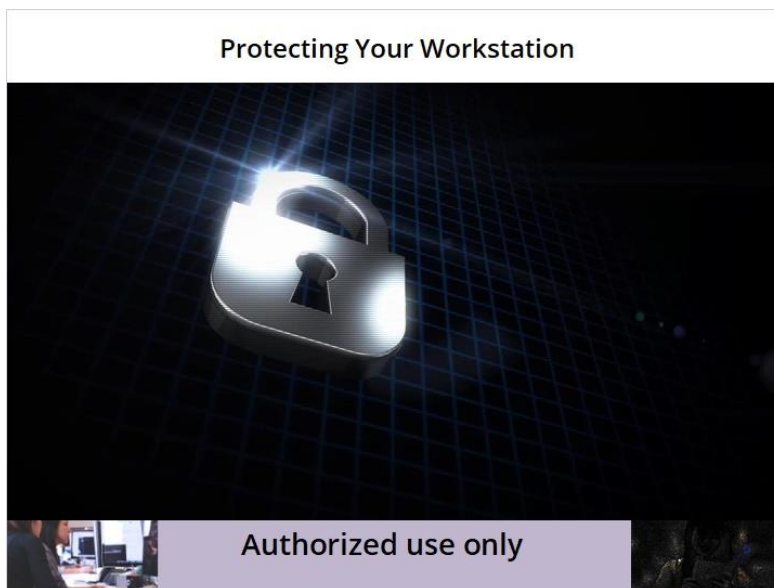
One of the best ways to keep information secure is to create strong passwords.

A good password is easy for you to remember but hard for someone else to guess.

The guidelines to create strong passwords include:

- The best passwords use a combination of numbers, upper and lowercase letters and special characters
- 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
- Do not use dictionary words

3.4 Workstation Protection



Narration:

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:

- Lock your workstation if you need to leave for any period of time.
- 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

3.5 Device and Laptop Protection

Protecting Your Mobile Device or Laptop	
Methods to Secure Mobile Device or Laptop	
Mobile Device	Laptop
Turn off Bluetooth discovery mode	Always use a docking station or laptop security cable
Avoid public Wi-Fi hotspots	Use a username and password to login to your laptop
Beware of text message spam	Setup an automatic log off after a pre-determined period of inactivity
Be selective with smart phone apps	Data encryption
Do not store passwords on your phone	Virus protection
Avoid check-ins, turn off geotagging	Symantec endpoint protection
Download security updates and back-up your data regularly	Antivirus application
If your mobile device is lost or stolen and contains sensitive consumer information, you must report it to your supervisor and Covered California immediately	

Narration:

You are responsible for the confidentiality and 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.

3.6 Travel and Remote Work



Travel and Working Remotely

- Carry your laptop with you, avoid setting your laptop or tablet on the floor
- Avoid using unsecure WiFi's to connect to your network
- Affix your name and contact info to laptops or tablets
- Use a Virtual Private Network (VPN)
- Disable file and printer sharing
- Make your folders private
- Use a personal firewall

Narration:

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

- Carry your laptop with you, avoid setting your laptop or tablet on the floor
- Avoid using unsecure WiFi's to connect to your network
- Affix your name and contact info to laptops or tablets
- Use a Virtual Private Network, or VPN
- Disable file and printer sharing
- Make your folders private
- Use a personal firewall

3.7 Email Security

Email Security Slow down, think and check before hitting "send" <ul style="list-style-type: none"> • Auto-complete • Copying and blind copying 	
The "Do's and Don'ts" of Email Security	
Do	Don't
Open emails only from people you know and trust	Provide your email, or someone else's email, address online
Open only those email attachments whose headings or texts sound familiar	Trust a site just because it claims to be secure
Use email encryption for particularly sensitive messages	Open email attachments containing the following file extensions: .exe, .bat, .reg, .scr, .dll, or .pif
Delete suspicious messages	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	Open emails addressed to people other than you
	Respond to emails that request your personal or financial information

Narration:

When using email, slow down, think and check before hitting "send."

Common mistakes include:

- Auto-complete: 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.


3.8 Sensitive Info through Email

Sending Sensitive Information over Email

A completed paper application must **NEVER** be sent via email

Any two pieces of information that identify a consumer 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



Narration:

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, for example the 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.

3.9 Protecting files

Password Protect and Encrypt Documents

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.



Narration:

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.

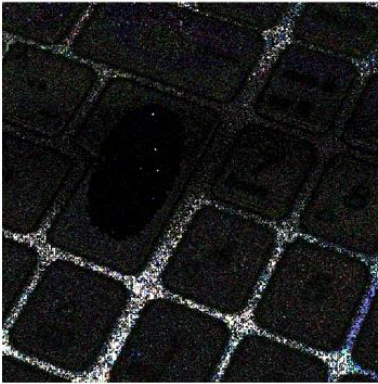
Steps to password protect in Microsoft Office:

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

Password Protect and Encrypt Documents

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.




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.

3.10 Social Media Safety

Social Media Safety

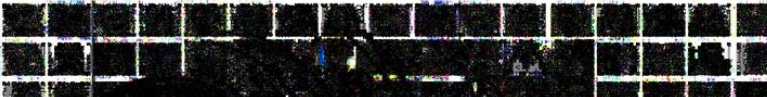


Hackers, spammers, virus writers, identity thieves, and other criminals follow the traffic on these sites

As social media usage grows so does the need to keep identity secure

Tips for social media protection:

- Create a social media-specific email
- Do not trust that a message is really from who it says it is from
- Be selective about whom you accept as a friend on a social network



Narration:

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.

Some tips for social media protection:

- Create a social media specific email
- Do not trust that a message is really from who it says it is from
- Be selective about whom you accept as a friend on a social network

3.11 Covered CA Requirements

Requirements to Protect Privacy and Security

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 name, address, Social Security number, financial records and health status.



Narration:

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 name, address, Social Security number, financial records and health status.

Requirements to Protect Privacy and Security

Keep Consumer Information Private

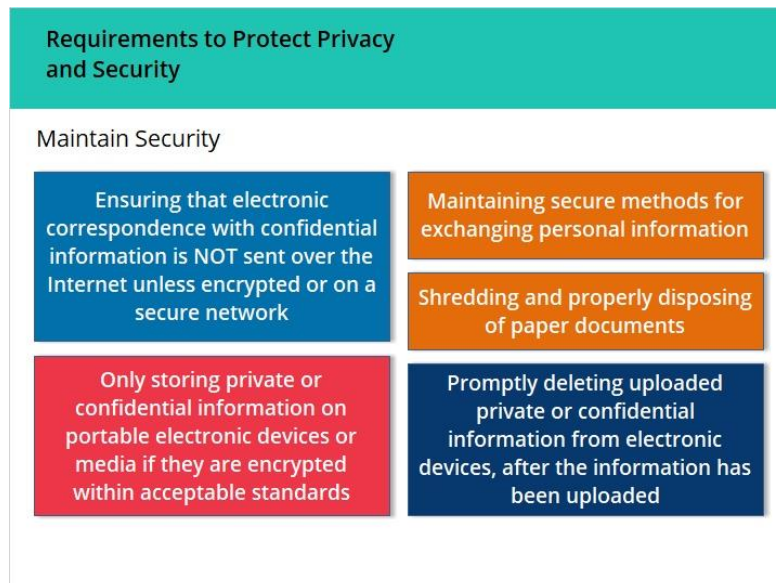
Use and discuss applicant information only when necessary for your role with Covered California	Do not disclose confidential information that violates the privacy rights of consumers
Do not share information with unauthorized persons	Do not request, store or disclose a consumer's CoveredCA.com username and password
Use applicant personal and health information only for the reasons it was intended, or as the applicant allows, or the law requires	Handle all applicant information and materials in a way that protects confidentiality and privacy

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 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 uploaded

4. Reporting Security and Privacy Incidents

4.1 Reporting Security and Privacy Incidents



Narration:

Reporting and Penalties

4.2 Reporting Security and Privacy Incidents

A man with dark hair and glasses, wearing a grey sweater, is shown in profile, looking down with his hands clasped in front of him, appearing to be in deep thought or listening intently.

Reporting Security and Privacy Incidents	
	No incident is too small or unimportant.
	If you have a concern or need guidance regarding a potential incident, seek one of the following resources:
	<ul style="list-style-type: none">• Your supervisor• Covered California
	Informationsecurity@covered.ca.gov PrivacyOfficer@covered.ca.gov
	Privacy Officer 1601 Exposition Blvd. Sacramento, CA 95815

Narration:

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.

If you have a concern or need guidance regarding a potential incident, seek one of the following resources:

- Talk to your supervisor who knows you and the details of your role with Covered California
- 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

4.3 Your Duty to Report

Your Duty to Report Suspected Incidents



You should **not** wait to confirm the incident happened, or to investigate what happened, but must immediately report any suspected incident.

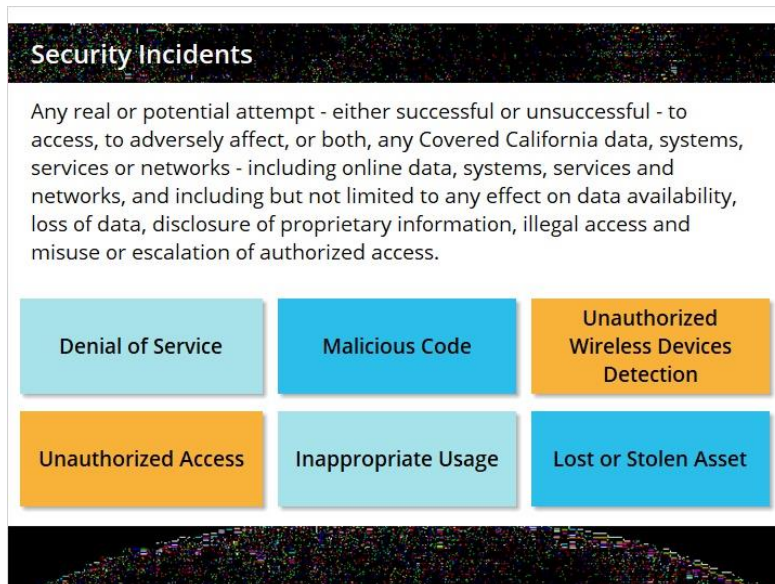
- When you report an incident, Covered California Information Privacy Office staff will then take immediate action to prevent harm and will direct you on what action to take
- This duty to report includes both privacy and security incidents

Narration:

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 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

4.4 Security Incidents

A graphic titled "Security Incidents" with a dark, pixelated background. It contains a definition of a security incident and six examples of incidents arranged in two rows of three boxes each. The top row includes "Denial of Service", "Malicious Code", and "Unauthorized Wireless Devices Detection". The bottom row includes "Unauthorized Access", "Inappropriate Usage", and "Lost or Stolen Asset".

Security Incidents

Any real or potential attempt - either successful or unsuccessful - to access, to adversely affect, or both, any 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.

Denial of Service	Malicious Code	Unauthorized Wireless Devices Detection
Unauthorized Access	Inappropriate Usage	Lost or Stolen Asset

Narration:

A security incident is defined as any real or potential attempt - either successful or unsuccessful - to access, to adversely affect, or both, any 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** - 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

4.5 Immediately Report



Narration:

You must **IMMEDIATELY REPORT** a suspected or actual security or privacy incident to your supervisor and contact the Covered California Privacy Office through email at

PrivacyOfficer@covered.ca.gov

Or by telephone at 1-800-889-3871

When you report an incident, a Privacy Office staff member will send you an Incident Report Form to fill out with basic information about the incident.

The Privacy Office alerts the Information Security Officer and other executive staff of the incident as needed, and forwards reports to them. The Privacy Office then directs you on next steps.

4.6 California State Law

Under applicable federal and California State law, Covered California contractors are required to abide by certain rules of behavior pertaining to the receipt, processing, storage and use of PII. These rules of conduct have been outlined within this training course.

By clicking “**Next**”, you acknowledge and agree that you have reviewed these requirements and will at all times abide by the privacy and security-related requirements covered by this training course.



Narration:

Under applicable federal and California State law, Covered California contractors are required to abide by certain rules of behavior pertaining to the receipt, processing, storage and use of PII. These rules of conduct have been outlined within this training course. By clicking “Next”, you acknowledge and agree that you have reviewed these requirements and will at all times abide by the privacy and security-related requirements covered by this training course.

5. Voter Registration

5.1 Mandatory Voter Registration Assistance



Narration:

Covered California Mandatory Voter Registration Assistance Training

5.2 Voter Registration Assistance

VOTER REGISTRATION ASSISTANCE

Mandatory

Under Federal and State law, Covered California must offer consumers voter registration services each time a person seeks service or assistance with:

- An application
- A renewal or re-enrollment of their application
- Change of address

If a consumer seeks help for one of the above reasons Covered California **must** offer help with voter registration to the same degree as is offered by the representative to complete Covered California's form, unless assistance is declined.



Narration:

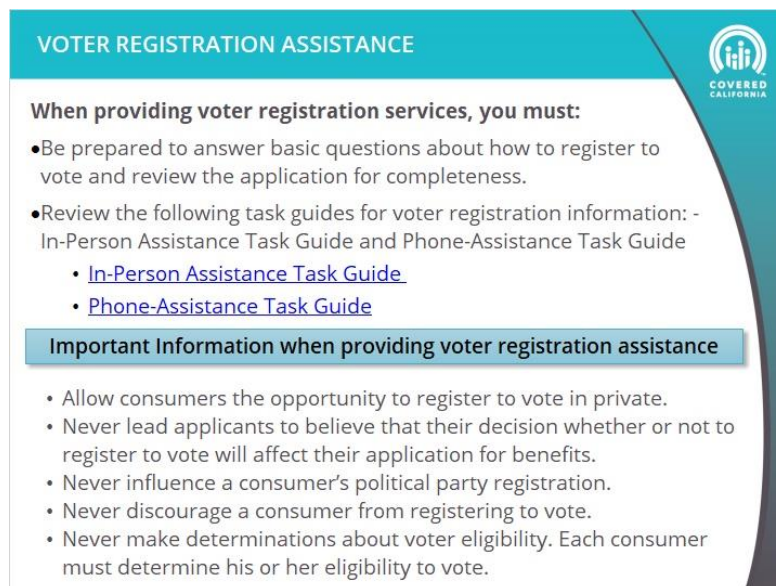
Mandatory

Under Federal and State law, Covered California must offer consumers voter registration services each time a person seeks service or assistance with:

- An application
- A renewal or re-enrollment of their application
- Change of address

If a consumer seeks help for one of the above reasons Covered California must offer help with voter registration to the same degree as is offered by the representative to complete Covered California's form, unless assistance is declined.

5.3 Voter Registration Assistance

A graphic titled "VOTER REGISTRATION ASSISTANCE" with the Covered California logo. It lists requirements for providing voter registration services and important information for providers.

VOTER REGISTRATION ASSISTANCE

When providing voter registration services, you must:

- Be prepared to answer basic questions about how to register to vote and review the application for completeness.
- Review the following task guides for voter registration information: - In-Person Assistance Task Guide and Phone-Assistance Task Guide
 - [In-Person Assistance Task Guide](#)
 - [Phone-Assistance Task Guide](#)

Important Information when providing voter registration assistance

- Allow consumers the opportunity to register to vote in private.
- Never lead applicants to believe that their decision whether or not to register to vote will affect their application for benefits.
- Never influence a consumer's political party registration.
- Never discourage a consumer from registering to vote.
- Never make determinations about voter eligibility. Each consumer must determine his or her eligibility to vote.

Narration:

When providing voter registration services, you must:

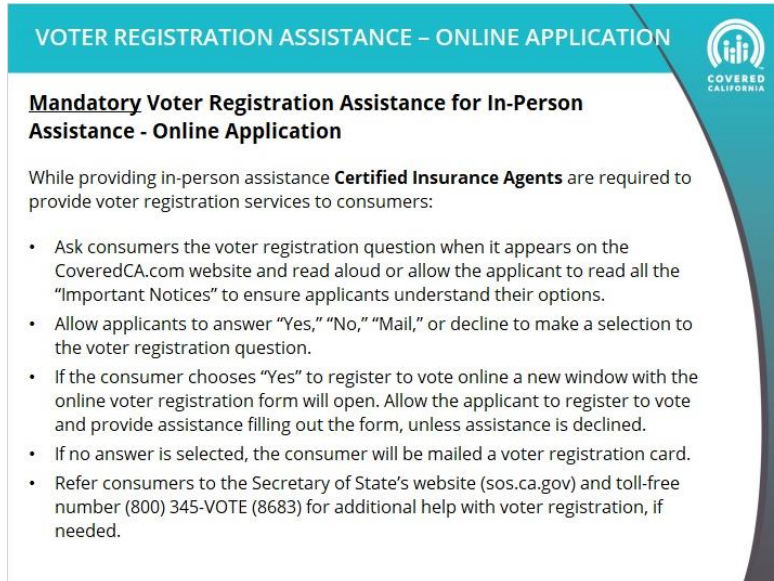
- Be prepared to answer basic questions about how to register to vote and review the application for completeness.
- Review the following task guides for voter registration information: - In-Person Assistance Task Guide and Phone-Assistance Task Guide

Voter registration assistance requirements:

- Allow consumers the opportunity to register to vote in private.
- Never lead applicants to believe that their decision whether or not to register to vote will affect their application for benefits.
- Never influence a consumer's political party registration.
- Never discourage a consumer from registering to vote.

- Never make determinations about voter eligibility. Each consumer must determine his or her eligibility to vote.

5.4 Voter Registration Assistance – online application



VOTER REGISTRATION ASSISTANCE – ONLINE APPLICATION

Mandatory Voter Registration Assistance for In-Person Assistance - Online Application

While providing in-person assistance **Certified Insurance Agents** are required to provide voter registration services to consumers:

- Ask consumers the voter registration question when it appears on the CoveredCA.com website and read aloud or allow the applicant to read all the "Important Notices" to ensure applicants understand their options.
- Allow applicants to answer "Yes," "No," "Mail," or decline to make a selection to the voter registration question.
- If the consumer chooses "Yes" to register to vote online a new window with the online voter registration form will open. Allow the applicant to register to vote and provide assistance filling out the form, unless assistance is declined.
- If no answer is selected, the consumer will be mailed a voter registration card.
- Refer consumers to the Secretary of State's website (sos.ca.gov) and toll-free number (800) 345-VOTE (8683) for additional help with voter registration, if needed.

Narration:

Mandatory Voter Registration Assistance for In-Person Assistance - Online Application

While providing in-person assistance, Certified Insurance Agents are required to provide voter registration services to consumers:

Ask consumers the voter registration question when it appears on the CoveredCA.com website and read aloud or allow the applicant to read all the "Important Notices" to ensure applicants understand their options.

Allow applicants to answer "Yes," "No," "Mail," or decline to make a selection to the voter registration question.

If consumer chooses "Yes" to register to vote online, a new window with the online voter registration form will open. Allow the applicant to register to vote and provide assistance filling out the form, unless assistance is declined.

If no answer is selected, the consumer will be mailed a voter registration card.

Refer consumers to the Secretary of State's website (sos.ca.gov) and toll-free number (800) 345-VOTE (8683) for additional help with voter registration, if needed.

5.5 Voter Registration Assistance – online application

VOTER REGISTRATION ASSISTANCE – ONLINE APPLICATION

Covered California makes voter registration quick and easy.



This is the Covered California voter registration page in the online application.

If consumers choose “Yes, open the California Online Voter Registration website,” the California Secretary of State’s Online Voter Registration page will open in a new window.

Narration:

This is the Covered California voter registration page in the online application.

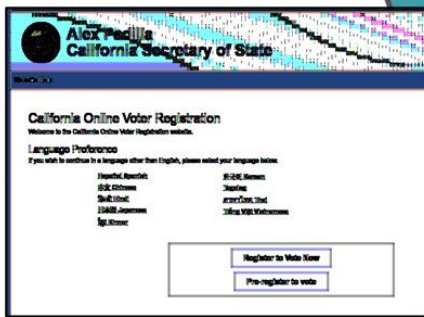
If consumers choose “Yes, open the California Online Voter Registration website,” the California Secretary of State’s Online Voter Registration page will open in a new window.

5.6 Voter Registration Assistance – Online Application

VOTER REGISTRATION ASSISTANCE – ONLINE APPLICATION

California’s Secretary of State’s Online Voter Registration Page

- Online voter registration is available in 10 languages.
- Allow consumers to select the language of their choice.
- Remember, a consumer has the right to register in private. Consumers must register to vote before they can vote, and must re-register to vote if they have moved or changed their name.
- If a consumer has a question you can’t answer, refer the consumer to the Secretary of State’s office at (800) 345-VOTE (8683) for additional help.



Narration:

California's Secretary of State's Online Voter Registration Page

- Online voter registration is available in 10 languages.
- Allow consumers to select the language of their choice.
- Remember, a consumer has the right to register in private. Consumers must register to vote before they can vote, and must reregister to vote if they have moved or changed their name.
- If a consumer has a question you can't answer, refer the consumer to the Secretary of State's office at (800) 345-VOTE (8683) for additional help.

5.7 Voter Registration Assistance – Paper Application

VOTER REGISTRATION ASSISTANCE – PAPER APPLICATION

Mandatory Voter Registration Assistance for In-Person Assistance - Paper Application

While providing in-person assistance Certified Insurance Agents are required to provide voter registration services to consumers:

- Read aloud or allow the applicant to read all the "Important Notices" to ensure applicants understand their options.
- Allow applicants to answer "Yes," "No," "Send," or decline to make a selection to the voter registration question.
- If the consumer wants to register to vote and Internet available, choose "Yes, I will go online" and take the consumer to <https://www.coveredca.com/resources/voter-registration/>. Select "Yes", then choose the registration form in the consumer's preferred language if it is offered and provide assistance filling out the form, unless assistance is declined.
- If the consumer wants to register to vote and Internet not available, choose "Yes, send me a voter registration form" and a card will be mailed to the consumer.

Narration:

Mandatory Voter Registration Assistance for In-Person Assistance - Paper Application

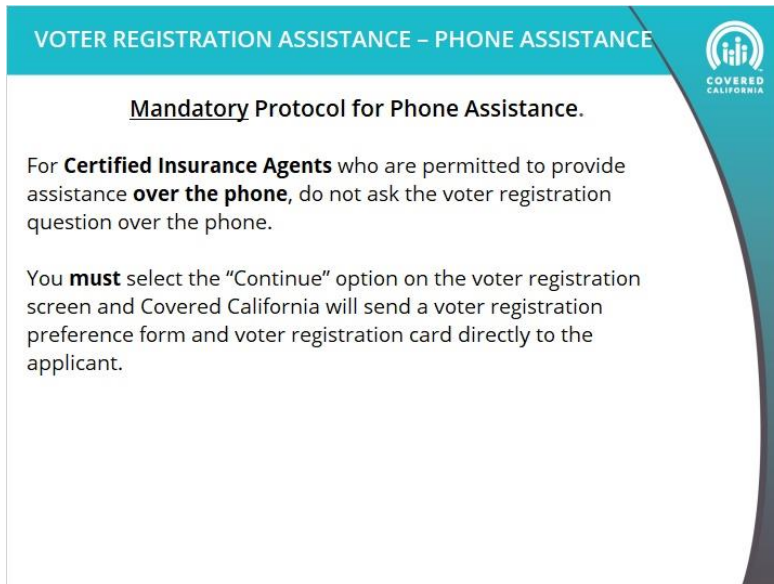
While providing in-person assistance Certified Insurance Agents are required to provide voter registration services to consumers:

- Read aloud or allow the applicant to read all the "Important Notices" to ensure applicants understand their options.
- Allow applicants to answer "Yes," "No," "Send," or decline to make a selection to the voter registration question.
- If the consumer wants to register to vote and internet is available, choose "Yes, I will go online" and take the consumer to the following link: <https://www.coveredca.com/resources/voter-registration/>. Select "Yes", then choose the registration form in the consumer's preferred language if it is offered

and provide assistance filling out the form, unless assistance is declined.

- If the consumer wants to register to vote and internet is not available, choose “Yes, send me a voter registration form” and a card will be mailed to the consumer.

5.8 Voter Registration Assistance – Phone Assistance

A graphic with a teal header and a white body. The header contains the text "VOTER REGISTRATION ASSISTANCE – PHONE ASSISTANCE" and the Covered California logo. The body contains the following text:

Mandatory Protocol for Phone Assistance.

For **Certified Insurance Agents** who are permitted to provide assistance **over the phone**, do not ask the voter registration question over the phone.

You **must** select the “Continue” option on the voter registration screen and Covered California will send a voter registration preference form and voter registration card directly to the applicant.

The graphic has a decorative curved line on the right side.

Narration:

Mandatory Protocol for Phone Assistance.

For Certified Insurance Agents who are permitted to provide assistance over the phone, do not ask the voter registration question over the phone.

You must select the “Continue” option on the voter registration screen and Covered California will send a voter registration preference form and voter registration card directly to the applicant.

5.9 Voter Registration Assistance

VOTER REGISTRATION ASSISTANCE

Certified Insurance Agents must review the In-Person Assister Procedure Task Guide for Voter Registration and Phone Procedure Task Guide available at: <http://hbex.coveredca.com/toolkit/webinars-briefings/>

[In-Person Assister Procedure Task Guide for Voter Registration](#)
[Phone Assistance Task Guide for Voter Registration](#)

The task guides include Frequently Asked Questions about registering to vote to prepare you to provide equal assistance with voter registration.


Regulations are found in the California Code of Regulations Section 6462. [Click here to access the regulations](#)

For additional information on voter registration you can contact the Secretary of State's Office:

Email: elections@sos.ca.gov

Website: <http://www.sos.ca.gov/elections/voter-registration/>

Or contact your county elections office.



Contact the Secretary of State:

(800) 345-VOTE (8683) - English	(800) 339-2957 - Tagalog
(800) 232-VOTA (8682) - español / Spanish	(855) 345-3933 - ภาษาไทย / Thai
(800) 339-2857 - 中文 / Chinese	(800) 339-8163 - Việt ngữ / Vietnamese
(888) 345-2692 - हिन्दी / Hindi	(800) 833-8683 - TTY/TDD
(800) 339-2865 - 日本語 / Japanese	(866) 575-1558 - 한국어 / Korean
(888) 345-4917 - ខ្មែរ / Khmer	

Narration:

Certified Insurance Agents must review the In-Person Assister Procedure Task Guide for Voter Registration and Phone Procedure Task Guide available by clicking this link: <http://hbex.coveredca.com/toolkit/webinars-briefings/>

Click these two links to find the:

In-Person Assister Procedure Task Guide for Voter Registration

And the:

Phone Assistance Task Guide for Voter Registration

The task guides include Frequently Asked Questions about registering to vote to prepare you to provide equal assistance with voter registration.

Regulations are found in the California Code of Regulations Section 6462. Click here to access the regulations.

[https://govt.westlaw.com/calregs/Document/I9D5776E22F17437192876D5043600414?viewType=FullText&originationContext=documenttoc&transitionType=CategoryPageItem&contextData=\(sc.Default\)](https://govt.westlaw.com/calregs/Document/I9D5776E22F17437192876D5043600414?viewType=FullText&originationContext=documenttoc&transitionType=CategoryPageItem&contextData=(sc.Default))

For additional information on voter registration you can contact the Secretary of State's Office:

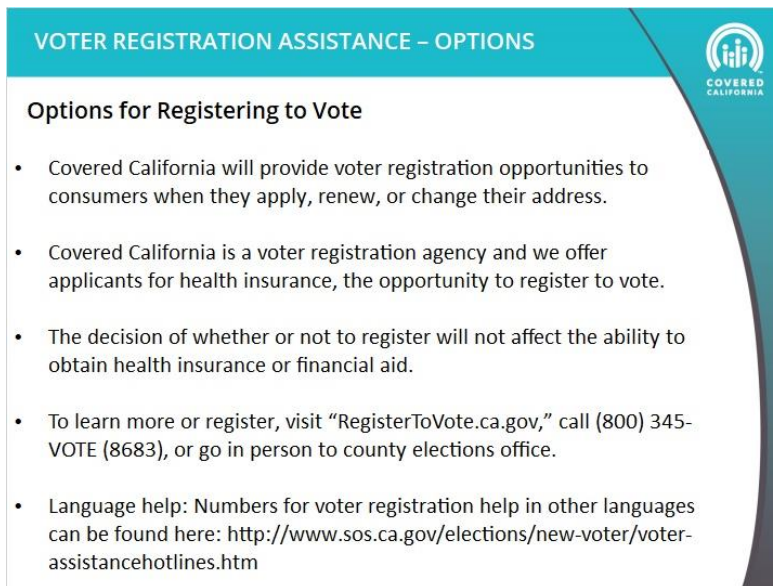
By Email at elections@sos.ca.gov

Or visit the Secretary of State's Website by clicking this link:

<http://www.sos.ca.gov/elections/voter-registration/>

You can also contact your county elections office.

5.12 Options

A presentation slide titled "VOTER REGISTRATION ASSISTANCE - OPTIONS" with the Covered California logo in the top right corner. The slide lists five bullet points under the heading "Options for Registering to Vote".

VOTER REGISTRATION ASSISTANCE - OPTIONS

Options for Registering to Vote

- Covered California will provide voter registration opportunities to consumers when they apply, renew, or change their address.
- Covered California is a voter registration agency and we offer applicants for health insurance, the opportunity to register to vote.
- The decision of whether or not to register will not affect the ability to obtain health insurance or financial aid.
- To learn more or register, visit "RegisterToVote.ca.gov," call (800) 345-VOTE (8683), or go in person to county elections office.
- Language help: Numbers for voter registration help in other languages can be found here: <http://www.sos.ca.gov/elections/new-voter/voter-assistancehotlines.htm>

Narration:

Options for Registering to Vote

Covered California will provide registration opportunities to consumers when they apply, renew, or change their address.

Covered California is a voter registration agency and we offer applicants for health insurance, the opportunity to register to vote.

The decision of whether or not to register will not affect the ability to obtain health insurance or financial aid.

To learn more or register, visit "RegisterToVote.ca.gov," call (800) 345-VOTE (8683), or go in person to county elections office.

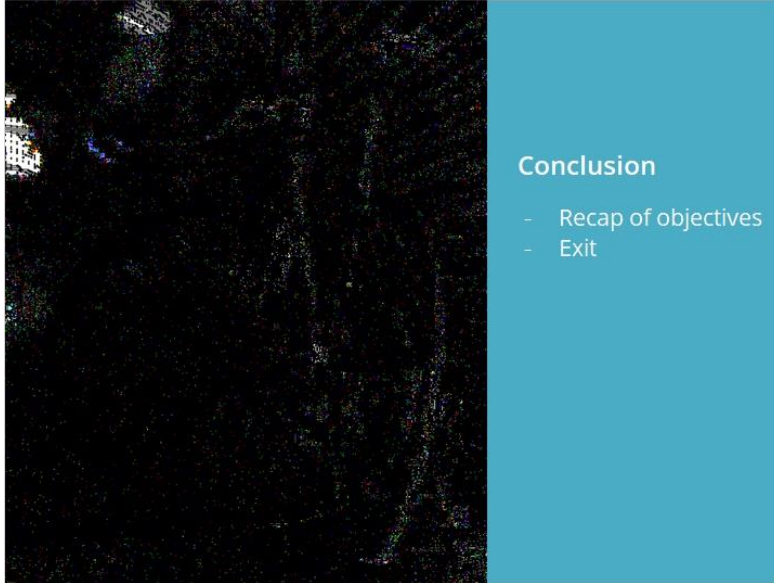
Language help: Numbers for voter registration help in other languages can be found at the link below.

For Certified Insurance Agents who are permitted to provide assistance over the phone, do not ask the voter registration question over the phone.

You must select the "Continue" option on the voter registration screen and Covered California will send a voter registration preference form and voter registration card directly to the applicant.

6. Conclusion

6.1 Conclusion



Narration:

Conclusion

- Recap of objectives
- Exit

6.2 Thank you

