



Confidential Data Handling Essentials

This document describes critical system and data user portions of the California Cancer Registry (CCR) Information Security Policy, available at www.CCRCal.org. CCR, Regional Registry staff, subcontractors and agents are responsible for following all portions of the policy, not just those highlighted below.

General Concepts

Appropriate Use

Equipment and services are for CCR work related uses only. CCR data should never be stored on personal or home use media or devices (PC, laptop, USB drive, CD, etc.).

Recognize CCR data (Confidential)

Under the statute that created the CCR, all data collected are considered confidential. This means that any information collected is considered confidential, regardless of format and medium, and needs to be protected from access by or disclosure to any unauthorized person. Patient information with personal identifiers like SSN, name, date of birth, address, etc. is the most critical.

Restrict access

Access to CCR data is allowed only to approved individuals and only to the minimum amount necessary to perform CCR work.

Protect the data

All CCR data need to be secured and protected appropriately to maintain confidentiality, no matter the medium. This means physical and electronic protections are required to prevent unauthorized access. Work related data requires encryption on any portable digital medium or device (laptop, USB drive, CD etc.)

Destroy when done

When data are no longer required, it must be properly destroyed.

Report any suspected loss

If there is a known or suspected loss of media or equipment, or known or suspected unauthorized access, report it immediately to your CCR supervisor or Regional Director.

Paper security

- Do not work with papers containing CCR data in view of unauthorized persons.
- Secure paper copies of CCR data in a labeled locked case and keep with you when transporting these data.
- Outgoing mailings must be double-enveloped with the inside envelope stamped “Confidential” and include who to contact if received in error. Mail should be sent by traceable means when feasible.
- Use locked storage for papers containing CCR data when these data are not in use.
- Shred paper copies of CCR data when no longer necessary.

Fax security

- Do not leave confidential information on a fax machine; watch over a fax machine while in use.
- Verify the recipient fax number before sending a fax.
- Use a cover sheet with full contact information and a confidentiality disclosure statement.
- Do not include confidential information on cover sheet.
- Send faxes only to monitored, secure fax machines.
- Send minimum amounts of CCR data necessary to perform CCR work.
- Verify receipt of fax by the intended recipient.
- Keep fax transmission logs as an audit trail.

Laptop / portable device security

Physical protection

- In an office - Laptops and other portable media must be locked to a desk or an immobile fixture during use, otherwise locked in a cabinet.
- On the road - When traveling, equipment is safest in your physical possession. Keep laptops with you at all times; do not leave laptops or other media with confidential information unattended in your car, airport, or a hotel room.
- At remote work sites – At sites such as a doctor’s office, keep laptops and media with you. Do not leave any equipment or materials unattended during breaks or overnight.
- At home - When not in use, store a laptop in a locked cabinet.

Passwords

- Use 8+ character, complicated (uppercase, lowercase, numbers and symbols), and not a dictionary word, name or familiar term. To create a password, consider using first letters of the words in a phrase, song, or rhyme that you know.

Encrypt confidential data

- Do not depend on Windows or other software application security; confidential data must be encrypted on any digital medium. For laptops use commercial grade whole drive encryption, like PGP Whole Disk, Drivecrypt, etc. For individual files in email, on servers, local hard drives, USB keys, CD’s, etc. use WinZip, TrueCrypt, or other commercial grade encryption program. Always use a strong password.

Keep software patched

- Windows and other software applications are updated and have security patches released often, and they need to be regularly patched and updated to current versions. Enable automatic updates or manually run manufacturers update program on a weekly basis to keep system updated and protected.

Antivirus / Spyware / Worm protection

- Ensure that high quality antivirus software that covers spyware and worms is installed and set to update signatures automatically. Weekly check to make sure the software is updated, functioning, and run a full system scan.

Firewalls (Internet/network connection security gatekeeper)

- In the office – Office networks must operate behind a firewall; firewalls are not required on individual machines.
- On the road or home – If the machine will connect to any network when outside the office, a local firewall needs to be enabled (Windows firewall or better).

Network connections

- Only connect to trusted networks.
- Any confidential data traveling over a network other than the internal Registry network requires encryption (VPN, HTTPS, etc.)

Wireless connections

- Due to the inherent insecurity of wireless connections, their use is not recommended for CCR work related activities.
- Configure wireless networks as securely as possible (see your owner's manual).
 - Run in infrastructure mode not ad-hoc or peer to peer.
 - Change SSID to long non-default name not related to you.
 - Disable broadcast of SSID.
 - Enable highest encryption available with a very long password (20+character) (best to worst – EAP/TLS, WPA2, WPA, WEP). WEP or no encryption should NOT be used.
 - Enable MAC address filtering.
- Disable wireless networks when not in use.

Machine Operations

- Run an operating system as a user, not as an administrator.
- Do not share laptop or other equipment with unauthorized persons (family and friends).
- Do not install any non-CCR work related applications. Use home machine for personal uses.

Web and Email use

Use care when surfing the web and opening e-mail.

- Use home machines for personal uses.
- Only visit reputable work-related sites.
- Only open messages from known sources and attachments that are verified.
- Backup data routinely in password-protected and encrypted formats.

Destroy CCR data when no longer needed.

- Machine and confidential digital media disposal requires a commercial grade data sanitization or zeroization application be run to fully remove/overwrite the data. File deletion or reformat are not good enough.

For Questions, Contact:

Regional Registry technical support or

Web www.CCRCal.org

Email ISO@ccr.ca.gov

Phone 916-779-2567