Appendix 4: Example Confidentiality Pledge

Employee Confidentiality Pledge

Confidentiality Protection Guidelines

Data collection, quality control, and research in which you will participate in one way or another are based upon the analysis of personal medical information on patients and research subjects. Therefore, the protection of such information is the responsibility of each member of the staff. As a staff member, you must understand that a breach of the confidentiality at any level is cause for immediate disciplinary action.

Responsibility for preserving confidentiality includes not merely passive acknowledgment of the procedures described below, but the active support of these procedures at all times. Accidental breaches will not be excused. Confidential information includes all patient, research subject, physician, and health care facility data. All such information is to be treated as medically privileged.

1. All employees are required to read and sign the *Employee Confidentiality Pledge* on their first day of employment and annually thereafter, and to abide by its guidelines. The *Employee Confidentiality Pledge* is then witnessed by the employee's supervisor. The Pledge is then placed in the employee's personnel file. Breach of this Pledge subjects the employee to immediate disciplinary action.

2. After signing the *Employee Confidentiality Pledge,* the employee is given a user name and password to log onto a network computer. If database access is required, a user name and password for database access will be assigned. All access passwords are considered confidential and are not to be shared.

3. Safeguards must be maintained to protect the medically sensitive and confidential information on all patients and research subjects whose information is contained in the California Cancer Registry databases. All cancer patient data are protected by the confidentiality requirements of the California Health and Safety Code, Sections 100330 and 103885. The confidentiality of medical information is further protected under provisions of the Government Code, Sections 6250-6265 (California Public Records Act). Provisions of the Civil Code, Section 1798–1798.70 (Information Practices Act), govern the release of personal identifiers or information that may allow identification of an individual. Therefore, personal identifiers as defined above should not be transmitted or published through e-mail, publications, presentations or any other public medium.

4. All files on patients and research participants are kept in locked file cabinets or in the locked confidential records room. Extra keys to staff file cabinets are to be available when needed but are to be kept inside the locked records room and never loose inside unlocked desk drawers. No confidential data should remain on top of desk after working hours. All lockable office doors should be closed and locked.

5. Office space will be secured and access to the premises limited to staff and authorized visitors. It is the responsibility of the staff member to make sure that no confidential data are visible to visitors.

6. All confidential data must be protected in a manner consistent with the current guidelines established by the institution and in accordance to requirements for access or use of CCR data.

7. A confidential fax cover sheet must be used when a staff member faxes confidential information. The recipient is to be notified in advance by telephone that confidential information is being transmitted, and the recipient should wait by the fax machine to retrieve the fax. The staff member should confirm that the fax has been received.

8. When mailing confidential information, staff members must place the confidential data inside an envelope, seal the envelope, stamp it "confidential," and place it in a mailing envelope. Also stamp "confidential" on the enclosed business reply envelope and on the mailing envelope.

9. When an employee is finished with computer printouts and other documents that contain confidential information, the documents are to be locked up or shredded.

10. Any breach of confidentiality must be reported immediately to your supervisor.

11. When employees are no longer employed by the institution, computer accounts (user ID and password) will be terminated and keys to buildings and offices will be returned to Administration. Terminated employees are admonished that their work has been confidential in nature, and this confidentiality should continue to be followed.

Confidentiality Protection Pledge

As a staff member of this institution, I give my personal assurance that I have read, understand, and will adhere to this *EMPLOYEE CONFIDENTIALITY PLEDGE.* I further understand that a breach of confidentiality, as described in the Pledge, is cause for disciplinary action.

_____	_____	_____
Staff Member (printed name)	Staff Member (signature)	Date

_____	_____
Supervisor	Date

Patient Data Confidentiality Guidelines

Help protect confidential data from unauthorized disclosure by:

In the Cubicle/Office

- Lock the computer by pressing the Windows + L key at the same time or by using CTL-ALT-DEL to bring up the Windows Security screen, and click on the “Lock Computer” button.
- Close confidential applications, such as Eureka, before you leave your cubicle/office for lunch or breaks.
- Face monitor away from the door to prevent viewing by unauthorized individuals.
- Keep all printed confidential data in confidential folders when not using it. Lock up all confidential folders with data when leaving the vicinity of your cubicle/office for more than a minute.
- Shred all printed confidential data when finished with it.
- Place all printed confidential data in folders and minimize all workstation screens containing confidential data when outside visitors are in your cubicle/office.

In the Break Room or Halls

- Do not discuss confidential data.
- Do not carry confidential data with you when using the break room or restroom.

In the Copy/Work Area

- Pick up all printouts promptly. If you walk by the printer, check any printouts of confidential data waiting to be picked up. If the owner can't be identified, place it in a confidential folder and give it to one of the administrative staff.
- Fax confidential data with a cover sheet marked "Confidential". Verify the fax number, send only to fax machines secured for confidential data, use the minimum amount of data possible, and make sure that somebody is waiting for the fax to arrive. For USPS or courier transport of confidential data, put the data in a sealed envelope marked "Confidential" with the recipient's name and then place the confidential envelope inside the mailing envelope. If digital media (CD, tape, USB drive) is being sent, encrypt the data with a strong password and send the password through other means.

Internet

- Use web browsing only for approved business uses
- Only open email from known trusted senders
- Verify email attachments with sender before opening
- Do not send confidential data over the Internet or email unless appropriately encrypted.

Computer

- Do not send or accept any data that is not appropriately encrypted.
- Use commercial grade encryption for email attachments, file transfer applications, laptop hard drives and other media like CD/DVDs, tape backup, USB keys, etc. that may contain confidential data. If possible encrypt confidential data on workstation and server drives.

- Remove all confidential data when no longer needed.
- Make sure that all OS and Office software security updates are applied.
- Use a commercial grade antivirus program and keep it up to date
- Follow IT guidelines for creating and changing workstation passwords.
- Memorize or carefully guard all passwords.
- Keep portable computers and storage media with you when travelling. Do not leave in cars, hotels or checked baggage.

Office Entry Doors

- Do not let anyone in the office you don't know, even if he/she appears to have an electronic key card.
- Do not prop open doors.
- Lock the front doors with the keys and set the alarm if you are the last one leaving the building.
- Instruct visitors to sign in and wear a visitor badge.
- Escort visitors back and forth to the door and instruct them to sign out and return the visitor badge.

Non-work Related Patient Look-up

- Do not do it.