TEXAS
Health and Human Services

Texas Department of State Health Services

Texas Cancer Registry

Confidential Information Security Policy

Texas Department of State Health Services
Cancer Epidemiology and Surveillance Branch
Texas Cancer Registry
August 2017

TABLE OF CONTENTS

Texas Cancer Registry
Confidential Information Security Policy
August 2017

PURPOSE

Cancer data are highly confidential. Improper disclosure of cancer data could result in emotional, psychological, and financial harm to patients and their families. One of the most important responsibilities of cancer registry professionals is to protect the confidentiality of cancer patient information.

Providing administrative, physical, and technical safeguards for the confidential data that the Texas Cancer Registry (TCR) receives and works with is critical to TCR's work. This document:

- speaks to the importance of maintaining the confidentiality and security of TCR data;
- outlines and establishes general procedures that all TCR staff and contractors must follow when collecting, transmitting, storing, and maintaining confidential information;
- discusses the types of and how cancer data can be shared;
- addresses administrative, physical, and technical safeguards;
- describes the action(s) required of the TCR in the event that confidential information is compromised; and,
- discusses the procedures the TCR will take when a suspected incident involving confidential information occurs.

BACKGROUND

The TCR collects demographic and disease information on cancer patients from health care providers, health care facilities, other registries, and via data linkages. TCR collects cancer data to support its efforts to protect and promote the health of the people of Texas using the principles of epidemiology to:

- understand the causes of adverse health conditions and exposures;
- identify human populations at risk; and,
- make recommendations to reduce or prevent adverse health conditions or exposures.

TCR customers and stakeholders trust and expect that the TCR and every employee in the TCR takes every precaution to protect information to

maintain patient confidentiality and the integrity of the TCR. All TCR staff are expected to handle confidential information in a professional manner that safeguards the privacy of individuals and the data the TCR collects and maintains.

The TCR proactively works to ensure that risks to data systems and confidential information are regularly evaluated and modified to meet changing needs and/or to resolve issues. These evaluations include, but are not limited to, system penetration testing, vulnerability assessment of computer systems, and physical safeguards.

Potential incidents involving confidential information disclosure can occur in many ways. These include, but are not limited to:

- accidental disclosure;
- abuse of access privileges;
- accessing information for profit;
- unauthorized physical intruders; and
- attempts to access information to damage surveillance systems and disrupt operations.

The TCR quickly responds to any potential incident involving confidential data to mitigate the effects of a potential release of confidential information and to put into place measures to prevent potential future recurrence.

The CDC reports that cancer registry data are especially valuable as they contain a wealth of personally identifying information that can be used for many illicit/illegal purposes. The ways they can be used include, but are not limited to:

- Identity theft. Full names, addresses, telephone numbers, social security numbers, birthdates, and other personal information provide criminals the keys to obtain credit and purchase goods and services fraudently;
- A person's medical history, including diagnoses, treatments, and prescriptions can be used to obtain prescription medication fraudulently to embarrass or blackmail the person, or to increase insurance premiums; and,
- Health care providers could use breached data to enhance their ability to analyze market share and perform studies on costs, charges, and clinical services, giving the provider a competitive advantage in the market.

Respecting and protecting the data the TCR collects is critical to the work of the TCR. Each TCR employee – as well as those that support the TCR must actively work to protect and maintain the confidentiality of TCR data. Our reporters, persons with cancer, and those that report to the TCR expect, deserve, and require it.

RESPONSIBILITY AND AUTHORITY

The TCR Branch Manager (Branch Manager) is responsible for the security of the TCR's confidential information and for ensuring compliance with this policy and the procedures and processes outlined. The Branch Manager may delegate certain responsibilities to other TCR staff. Each TCR team member, contractor, and others working with TCR data, must understand and follow the laws, rules, policies, and procedures outlined in this document.

STATUTES AND RULES RELATED TO TCR SECURITY AND CONFIDENTIALITY

Many state and federal statutes, rules, and guidelines establish the TCR's authority and responsibility regarding confidential information. All staff should be familiar, understand, and follow the guidelines outlined in this policy. The list provided below provides enhanced detail relative to security and confidentiality.

- Texas Cancer Incidence Reporting Act, Chapter 82, Texas Health and Safety Code (http://www.statutes.legis.state.tx.us/Docs/HS/htm/HS.82.htm)
- Medical Records Privacy, Chapter 181, Texas Health and Safety Code (http://www.statutes.legis.state.tx.us/Docs/HS/htm/HS.181.htm)
- Texas Administrative Code Title 25, Health Services, Chapter 91, Subchapter A (Cancer Registry) https://texreg.sos.state.tx.us/public/readtac$ext.ViewTAC?tac_view=4&ti=25&pt=1&ch=91
- Texas Administrative Code Title 1, Administration, Part 10, Chapter 202, Subchapter B (Security Standards for State Agencies) https://texreg.sos.state.tx.us/public/readtac$ext.ViewTAC?tac_view=4&ti=1&pt=10&ch=202
- Texas Government Code, Chapter 552 (Public Information) http://www.statutes.legis.state.tx.us/Docs/GV/htm/GV.552.htm
- Texas Government Code, Chapter 2054, Subchapter F (Information Resources)

http://www.statutes.legis.state.tx.us/SOTWDocs/GV/htm/GV.2054.htm

- Texas Business and Commerce Code, Chapter 521 (Unauthorized Use of Identifying Information) http://www.statutes.legis.state.tx.us/Docs/BC/htm/BC.521.htm
- Health Insurance Portability & Accountability Act of 1996 (HIPAA), Public Law 104-91, https://aspe.hhs.gov/report/health-insurance-portability-and-accountability-act-1996
- Health Insurance Portability & Accountability Act of 1996 (HIPAA) Privacy Standards, 45 C.F.R. Parts 160 and 164. http://www.hhs.gov/hipaa/for-professionals/privacy/
- Health Information Technology for Economic and Clinical Health (HITECH) Act, Public Law 111-5, Division A, Title XIII (Health Information Technology), Subtitle D (Privacy), Part 1 (Improved Privacy Provisions and Security Provisions) and Part 2 (Relationship to Other Laws) http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/hitechact.pdf
- Veteran's Benefits; General Administrative Provisions; Records and Investigations; Records; Confidential Nature of Claims, 38 U.S.C 5701 (f) https://www.gpo.gov/fdsys/granule/USCODE-2010-title38/USCODE-2010-title38-partIV-chap57-subchapI-sec5701
- Veteran's Benefits; Boards, Administration, and Services: Veterans Health Administration – Organization and Functions; Protection of Patient rights; Confidentiality of Certain Medical Records, 38 U.S.C. 7332 http://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title38-section7332&num=0&edition=prelim
- Defense Manpower Data Center (DMDC) 02 Department of Defense, Defense Enrollment Eligibility Reporting System, 9 August 2009, 74 FR 39657 https://www.gpo.gov/fdsys/granule/FR-2009-08-07/E9-18894
- Health and Human Services Commission, Information Security/Cybersecurity Policy Circular C-021; https://hhs.texas.gov/about-hhs/leadership/policy-circulars-bulletins

The TCR is not exempt from HIPAA. The TCR complies with all HIPAA standards that apply to protected health information (PHI). HIPAA permits covered entities to disclose PHI, without authorization if it meets a statutorily defined use or disclosure. These types of permitted disclosures include the disclosure to public health authorities or other entities that are legally authorized to receive such reports for the purpose of preventing or controlling disease, injury, or disability. This includes the reporting of

disease or injury for conducting public health surveillance. The rule also permits PHI disclosures without a written patient authorization for specified public health purposes to public health authorities legally authorized to collect and receive the information. To comply with HIPAA standards for cancer reporting, the TCR may only collect reportable cancer cases and data items specified in the Cancer Reporting Law, Rules, and the TCR Cancer Reporting Handbook.
(https://www.dshs.texas.gov/tcr/reporting/hospitals.aspx)

AGREEMENTS RELATED TO TCR SECURITY AND CONFIDENTIALITY

The TCR enters into agreements with many other entities that provide additional requirements for the use of cancer data. The agreements are periodically reviewed and updated. The agreements provide additional requirements for TCR confidential information and include, but are not limited to:

- North American Association of Central Cancer Registries (NAACCR) National Data Exchange Agreements (the majority of states have this agreement) (https://www.naaccr.org/national-interstate-data-exchange-agreement/);
- Interstate Data Exchange agreements with Arizona, Florida, Kansas, Maryland, Missouri, Nevada and New Mexico (until and unless those states file a NAACCR National Data Exchange Agreements);
- National Death Index, National Center for Health Statistics, Centers for Disease Control and Prevention (https://www.cdc.gov/nchs/ndi/index.htm);
- Veteran Health Administration (VHA) Agreements with Texas VA Medical Centers;
- US Department of Defense, Defense Manpower Data Center Memorandum of Understanding.

POLICIES RELATED TO TCR SECURITY AND CONFIDENTIALITY

The TCR, the Department of State Health Services (DSHS), the Health and Human Services Commission (HHSC) also maintain policy and guidelines related to information security and confidentiality that TCR must follow. These include:

- TCR *Confidential Information Security Policy (https://www.dshs.texas.gov/tcr/lawrules.aspx);*
- TCR *Data Release Policy* (https://www.dshs.texas.gov/tcr/data/policy.aspx);

- TCR, *Quality Assurance Policy and Procedure Manual* (Confidentiality Policy for TCR Employees and Visitors; Shredding of Manual Forms; Out of State Cases; Instructions for Requesting An Authorization for Release of Medical Records);
- TCR, *Cancer Reporting Handbook* (Standards for Confidentiality, Disclosure of Data, and Quality Assurance; Reporting Tools) (https://www.dshs.texas.gov/tcr/publications.aspx);
- Texas Department of State Health Services, Policy Number IR-2204, Information Security Policy (http://online.dshs.state.tx.us/content.aspx?id=4819);
- *DSHS Information Security Standards and Guidelines* (associated with IR2204, Information Security Policy) (http://online.dshs.internal/it/standards/default.htm);
- *DSHS Computer Incident Response Plan;*
- *Veterans Health Administration Handbook* 1605.1, Paragraph 28. Registries (http://www.va.gov/vhapublications/, search for 1605.1);
- Health and Human Services Acceptable Use Agreement (AUA) (http://hhscx.hhsc.texas.gov/sites/extranet/files/docs/it/forms/hhs-aua.pdf);
- HHS Enterprise Information Security Standards and Guidelines (multiple documents located at http://hhscx.hhsc.texas.gov/it/policies-and-guidelines) ; and,
- HHSC Security Incident Management Plan (http://hhscx.hhsc.texas.gov/sites/extranet.dd/files/docs/it/policy/sec-standards-guidelines.pdf.

Remember – It is every TCR employee, contractor, or other persons using TCR data responsibility to understand, follow, and adhere to the information contained in this document. If you have a question, it is your responsibility to seek the advice and direction of your manager. If in doubt, ask!

DEFINITIONS

The definitions below are included to help readers of this document better understand its contents.

Breach of Confidential Information: the unauthorized acquisition, access, use or disclosure of protected health information (PHI) which compromises the security or privacy of the health information such that the use or disclosure poses a significant risk of financial, reputational, or other harm to

the affected individual, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information (Sec. 13402 Health Information Technology for Economic and Clinical Health (HITECH) Act).

Breach of System Security: the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by a person, including data that is encrypted if the person accessing the data has the key required to decrypt the data. Good faith acquisition of sensitive personal information by an employee or agent of the person for the purposes of the person is not a breach of system security unless the person uses or discloses the sensitive personal information in an unauthorized manner (Sec. 521.053 Business and Commerce Code).

CD; CD-W; CD-R: compact disk; write-only compact disk (one-time write capability only); re-writable compact disk (multiple read and write capability, like a diskette).

Confidential information: a) demographic and/or cancer diagnosis and treatment information that would or could result in the identification of the individual, treating physician or reporting institution should that information be released **b)** information that is excepted from disclosure requirements under the provisions of the Texas Public Information Act or other applicable state or federal law **c)** any information by which the identity of a client or employee can be determined either directly or by reference to other available information if the identity cannot be disclosed under federal or state law. For the purposes of this policy "confidential information" includes individually identifiable health information (IIHI), protected health information (PHI) and sensitive personal information (SPI). Confidential data items collected and/or maintained by the TCR include, but are not limited to, city of residence; street Address; ZIP Code; census tract; latitude; longitude; date of birth; last, first, and middle name; maiden name; suffix (i.e., name suffix); Social Security Number; Facility ID; Medical Record Number; and any other collected data item that, when used in conjunction with medical or epidemiologic information, could lead to identification of individuals, healthcare facilities, clinical laboratories or healthcare practitioners.

Electronically: the transfer of data by means of media (diskettes, CDs, USB flash drives or similar data storage devices) or the interconnection of two or more computers or computer systems by cable, wireless signal, satellite, telephone line, or any other communication medium with the capability to transmit information among the computers (network).

File Transfer Protocol (FTP): a protocol used on the Internet for exchanging electronic files.

Incident Involving Confidential Information (Confidential Information Incident): Any event that may involve the possible unauthorized release or access to confidential information in violation of the TCR Confidential Information Security Policy, state or federal law.

Individually Identifiable Health Information (IIHI): information that is a subset of health information, including demographic information collected from an individual, and: (a) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (b) relates to past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, future payment for the provision of health care to an individual; and that: identifies the individual or reasonably can be used to identify the individual. (45 C.F.R. Sec. 160.103)

Personnel Action (Failure to Comply): a TCR employee or temporary employee or volunteer who unintentionally causes an incident involving confidential information will be held accountable, and may be subject to counseling, additional confidentiality training and or disciplinary action, up to and including termination. A TCR employee or temporary employee or volunteer who intentionally causes an incident involving confidential information will be held accountable and disciplinary action may result up to and including termination. Some circumstances may warrant legal action and criminal penalties for failure to maintain required confidentiality.

PGP Encryption: Symantec software product deployed at the workstation and server levels that encrypts and decrypts data in transit and at rest.

Protected Health Information (PHI): information the Privacy Rule protects, including individually identifiable health information transmitted by electronic media or maintained in any medium and excludes education records and employment records. (45 C.F.R. Sec. 160.103)

Removable Media: data storage devices that can be accessed by plugging into a computer's USB port or card reader slot, including but not limited to pen drives, thumb drives, flash drives, memory sticks, and memory cards (compact flash, secure digital and smart media).

Risk Analysis: the process of identifying and documenting vulnerabilities and applicable threats to information resources.

Risk Assessment: the process of evaluating the results of the risk analysis by projecting losses, assigning levels of risk, and recommending appropriate measures to protect information resources.

Secure FTP (SFTP): Also known as "SSH (Secure Shell) File Transfer Protocol." A network protocol providing file transfer and manipulation over a secure data stream.

Secure HTTP (S-HTTP): a protocol for transmitting data securely over the Internet.

Secure Socket Layer (SSL): a protocol developed by Netscape for transmitting private documents via the Internet.

Security Plan: the framework within which an organization establishes needed levels of information security controls to achieve its desired information security goals.

Sensitive Personal Information (SPI): an individual's first name, or first initial and last name in combination with any or one of the following items, if the names and items are not encrypted: (a) social security number, (b) driver's license or government-issued identification number, or (c) account number, or credit or debit card number in combination with any required security code, access code or password that would permit access to an individual's financial account. Any information that identifies an individual and relates to: (d) the physical or mental health or condition of the individual, (e) the provision of health care to the individual, or (f) payment for the provision of health care to the individual. (Chapter 2054, Subchapter F, Texas Government Code and Sec. 521.002 Business and Commerce Code).

Visitor: any person other than a TCR employee, temporary employee, contractor, or volunteer who visits a TCR facility.

APPLICABILITY

The policy applies to anyone who accesses or receives TCR data. Anyone who access or receives TCR data must read, understand and comply with all confidential information and non-disclosure policies, procedures, and practices. **This documents supplements, and does not replace any policies, procedures, and practices regarding the same or similar matters issued by the HHSC and the DSHS.**

CONFIDENITALITY AND NON-DISCLOSURE AGREEMENT

New hires, temporary employees, contractors, volunteers, interns, and those visitors who will be allowed access to confidential information, and others as determined by the Branch Manager, must read, understand and comply with this policy. Each employee must:

- complete the TCR Confidentiality and Non-Disclosure Agreement form (available on the TCR SharePoint site);
- complete the Health and Human Services Acceptable Use Agreement (HHS AUA) found at http://hhscx.hhsc.texas.gov/sites/extranet/files/docs/it/forms/hhs-aua.pdf .
- review this policy in a conversation with their manger and or the Core Business Operations (CBO) manager;
- return the form to the TCR Administrative Assistant; and
- adhere to the TCR and HHS confidentiality of information and non-disclosure policies during their TCR employment and after cessation of employment or discontinuance of a person's business or educational relationship with the TCR.

Each TCR manager must:

- upon separation of a TCR employee, it is the supervising manager's responsibility to:
    - review the Confidentiality Forms and Agreements spreadsheet ..\..\..\Shared\Admin\Confidentiality Agreement\Confidentiality Forms and Agreements.xls to determine if any notifications to terminate access must be made and notify the TCR administrative assistant to make necessary changes and ongoing updates;
    - upon identification of a need to terminate access, the supervising manager must provide such notice (in writing) to the appropriate entity within three (3) business days of the employee's last physical day on the job;
    - the TCR CBO manager, or designee, must review the Confidentiality Forms and Agreements spreadsheet quarterly to confirm that the supervising manager has sent notices to terminate access; and,
    - print out and attach the termination of access notices to the appropriate form or agreement in the central office files.

The CBO area will review the spreadsheet at least annually to determine if any other additions and/or changes need to be made, however it is the supervising manager's primary responsibility to review the spreadsheet upon an employee leaving TCR.

RETENTION AND TERMINATION OF CONFIDENTIALITY AGREEMENTS

The TCR Administrative Assistant will:

- maintain a copy in central office files of all confidentiality and non-disclosure agreements, limited use data agreements, computer security access requests ,and similar documents and forms relating to confidentiality, security, and non-disclosure of confidential information; and,
- enter the appropriate information in the Confidentiality Forms and Agreements spreadsheet . ..\..\..\Shared\Admin\Confidentiality Agreement\Confidentiality Forms and Agreements.xls

The TCR CBO manager will:

- ensure that every new hire, temporary employee, contractor, volunteer and/or visitors who will be allowed access to confidential information has completed the TCR Confidentiality and Non-Disclosure Agreement and the Health and Human Services Acceptable Use Agreement (HHS AUA form.

TRAINING

All new hires, temporary employees, contractors, volunteers, visitors and others who will be allowed access to confidential information will receive training upon employment (within the first 5 (five) business days) and periodically thereafter. The training includes, but is not limited to:

- explanation of the reasons for confidentiality of information maintained by the TCR;
- instruction and guidance on TCR and HHS policies, procedures, and practices regarding the handling and protection of confidential information;
- review of applicable confidentiality rules and requirements; and,
- updates made to the policy or guidelines related to confidentiality and security.

Each TCR manager is expected to provide a general and job specific orientation to confidential and security policies, practices, and guidelines

during the first two days after a new employee or other person (contractor, volunteer, etc.) starts with the TCR. The TCR CBO Manager will provide a more in-depth orientation during the first five calendar days of the employee's, etc. start date in either a group or individual setting or upon the request of the manager (if the need for a repeat training is identified).

Each TCR employee is encouraged to periodically review this document to clarify their understanding and/or to address questions they may have. The Core Business Group Manager will also provide an annual training and update for all TCR staff.

Each TCR staff member is also required to complete all HHSC trainings related to confidentiality and security. These include but are not limited to computer usage and HIPPAA related trainings.

When in doubt, an employee must consult with their manager!

RISK MANAGEMENT

The TCR must ensure, working in collaboration, with Information Technology staff, that the risk to systems and confidential information is assessed regularly. Information security risk analyses are required at least biennially under Title 1, Part 10, Chapter 202, Subchapter B, 202.22 of the Texas Administrative Code (https://texreg.sos.state.tx.us/public/readtac$ext.ViewTAC?tac_view=5&ti=1&pt=10&ch=202&sch=B&rl=Y)

The TCR will ensure that DSHS IT:

- conducts a penetration test on each server used by the TCR;
- conducts a vulnerability assessment of its cancer surveillance database system using a currently approved assessment tool; and,
- initiates, completes and implements a mitigation plan to address any vulnerabilities identified.

TCR managers, or their designee, on a periodic basis, will conduct the following reviews and activities to ensure that the following activities occur periodically as noted:

- Quarterly:
    - conduct desk reviews to determine if staff is correctly securing confidential information;
- Annually:

- ensure that all case reporting forms and copies of medical records are shredded (or placed in special confidential shred containers) after entry into the TCR database but no more than one year from date of receipt;
- ensure that electronic copies are securely destroyed;
- provide security reminders to employees and cancer reporters ; and,
- review with their staff members procedures for receiving, sending and maintaining confidential information.

If a manager identifies a deficiency or a gap in knowledge, they must provide additional training and/or direction to the employee.

The TCR CBO Manager must, on at least an annual basis:

- review and update plans to protect equipment and data from fire and other hazards;
- review and update security measures to ensure confidential information is not used in a manner other than as authorized in the Texas Health and Safety Code, Chapter 82, the Texas Administrative Code (25 TAC 91) and other applicable laws or rules;
- review the list of persons with electronic key card access to the Austin TCR offices to ensure only approved individuals are included; and,
- validate account and password lists for TCR servers and databases to ensure that only approved individuals have access.

PHYSICAL SAFEGUARDS

Every TCR employee, contractor, and others who have or will have access to confidential information has a responsibility to keep it safe and secure.

Physical safeguards that must be followed to protect confidential information include, but are not limited to the following:

- keeping all confidential information, electronic and paper in a secure locked area with limited access;
- keeping all confidential information on a desktop or other computer screen out of view when persons not authorized to see the material are in the immediate vicinity;
- When traveling with confidential information:

    - transport all confidential information in a secure container (i.e. a locked briefcase);
    - ensure that the secure container is not visible when it is in a car, etc.;
    - ensure that when transporting electronically stored confidential information that the data is encrypted and password protected;
    - not leave any confidential information in any place or area where unauthorized persons may reasonably gain access;
    - not take any confidential information to a private residence, place of business (other than the facility that provided that information), or any other location outside of the transport vehicle;
- shredding or putting in a confidential recycle container all waste containing confidential information;
- controlling visitors and others access to TCR facilities and offices by ways that include, but are not limited to, the following:
    - making sure that visitors sign the Visitors Log (maintained in the front reception area);
    - escorting and accompanying , at all times, visitors to the TCR;
    - limiting visitors to TCR facilities and offices only for business purposes;
    - report lost or stolen access cards immediately;
    - keeping (and do not loan) keys and access cards secure;
    - keeping all TCR secured outside access doors closed (do not prop open or disable a door without approval of the Branch Manager or designee); and
    - Immediately reporting to a manager any visitor who is not authorized to be in the space. (Please note – DSHS facility and IT employees have authorized access to our offices to conduct the work they need to do).

TCR CBO staff routinely works with DSHS facilities staff to ensure that all physical security systems comply with state regulations and building and fire codes.

If a TCR employee suspects or knows that any device that may contain confidential information is missing or is believed to be missing or stolen, the employee must immediately report it to their manager and/or Branch Manager. The TCR will handle this as a possible privacy incident. As

appropriate, the manger will notify IT so that the device can be remotely wiped (if possible). A police report may need to be filed.

COMPUTER AND ELECTRONIC SAFEGUARDS

Maintaining the security of electronic data containing confidential information is also critical to the work of the TCR. TCR staff or those providing information security activities must understand, observe, and comply with the following:

- storing all data files on a network drive to ensure the backup of files; data files are not to be saved on a workstation's hard drive;
- using passwords:
    - use a unique UserID and strong secret password to log onto the computer network;
    - change your password every 60 days;
    - keep your password confidential (do not share it, do not write it down, and do not attach it to the piece of equipment);
    - password protect (at the Windows login level) all desktop, laptop, notebook, tablet computers;
- have access only to those systems and drives for which access is needed for a business purpose (the principle of least privilege);
- use screen savers:
    - set up and activate password protected screen savers that automatically start after ten (10) minutes of inactivity;
    - activate screen savers if confidential information is on the screen and the user will be away from their desk;
- ensure that all data files with confidential information are encrypted and password protected;
- restart (not shut down) all workstations at the end of the work day unless instructed otherwise by DSHS IT. Exceptions to this may be granted by the employee's manager if there is a business need to run programs overnight and/or to facilitate security updates. If the exception is approved, the workstation must be placed in "locked" mode and rebooted the next workday to ensure the installation of security updates;
- not use external ports on workstations that will accommodate removable media devises (such as flash and thumb drives). Each is disabled and must remain disabled unless the Branch Manager

approves such use in writing for business reasons (note: most computers within the TCR have this functionality already disabled);

- protect all workstations using PGP encryption software (installed by DSHS IT);
- work with IT to ensure that the appropriate security settings are in the Registry Plus Software;
- ensure that all servers containing TCR test and production databases and all networks drives with confidential information are encrypted using PGP encryption software or other server encryption as determined by DSHS IT;
- enable the cover page feature when printing documents to avoid confidential information being mixed into/with other print jobs; and,
- use approved machines to send and receive faxes containing confidential information, only when permissible to do so (CBO staff will ensure that those machines are located in secure areas of the central and regional offices).

Staff should use removable media devices (such as USB flash drives and thumb drives) only for the reasons listed below. All other uses are prohibited.

- Accommodate the needs of external partners as long as the following are met:
    - Requestor:
        - provides a valid reason for not using the Web Plus server;
        - verifies that the requestor's agency has a policy in place that allows removable media devices meeting at least the FIPS 140-2 security requirements for cryptographic modules;
        - provides a FIPS 140-2 Validation Certificate from the NIST for the devise to be used;
        - Requestor provides the removable media devise and directions for its use; and,
- Branch Manager provides written approval for the exception.

Shared user accounts are prohibited, but the Branch Manager may grant written permission if a business need warrants a shared account. The supervising manager in the TCR area that needs such access must submit a written request to the Branch Manager requesting approval. The request must include:

- the application(s), system(s) and network(s) that the shared account will be used for;
- the names of the TCR staff member(s) or other authorized user who will share the account;
- a brief explanation of the business need for the shared account; and assurances that the system audit log(s) are able to identify individual users or detail on why capturing such information is not necessary and will not create a system vulnerability or security risk; and,
- the length of time for which such shared accounts will be in use.

TCR managers with staff who have shared user accounts are responsible for terminating access as appropriate.

In the event that confidential information is stored and transported on laptop, notebook, or tablet computers the information must be downloaded to a secure network drive on the day of the return to the office, or no later than the next business day unless the timeframe is approved by the staff member's manager. Once the confidential information is downloaded the hard drive must be sanitized to ensure the removal of all confidential information. Sanitation of the laptop or similar mobile device must be:

- done using a DSHS IT approved sanitation software and following DSHS sanitation procedures;
- done by the TCR Systems Analyst upon return of the device and before the device is returned to inventory. In the regions, two staff members (a primary and a backup) are designated by their manager as responsible for ensuring that computer hard drives are sanitized before the computer is used again. The TCR System Analyst will ensure that the designated regional staff are trained and receive assistance on the use of proper sanitation software and procedures; and,
- prior to the disposal or re-use of removable media containing confidential information staff will consult with the TCR Systems Analyst about the current method(s) to sanitize the device and will implement those methods and procedures. Staff are reminded that merely deleting files only clears the file allocation table and does not remove the data.

***********Confidential data must NEVER be accessed on any computer that does not meet HHS IT Security Requirements**********

Texting should never be used for any communication involving protected health information.

EXCHANGE OF CONFIDENTIAL DATA

Cancer data must only be released when the release in accordance with TCR policies, practices, and guidelines.

The following policies and procedures apply to the exchange and transmission of confidential data:

- requests for release of confidential information must be approved by the Branch Manager, the DSHS Institutional Review Board (IRB), and by the DSHS Research Executive Steering Committee (https://www.dshs.texas.gov/irb/default.shtm);
- the TCR Epidemiology Group must handle all requests for statistical data/information;
- TCR operations staff will respond to all requests related to patient listings and accession registers that are compiled and shared with the original reporting entity in order to facilitate quality assurance activities;
- requests for non-confidential data/information will be reviewed by the TCR Epidemiology Group to ensure that the data can be provided in accordance with TCR's data release policy for such data (https://www.dshs.texas.gov/tcr/data/policy.aspx);
- researchers or facilities requesting data or wanting to perform data linkages with the TCR must complete and follow the procedures outlined in the TCR Data Release Policy (https://www.dshs.texas.gov/tcr/data/policy.aspx);
- all de-identified data sets prepared for public use and research purposes must be reviewed by the TCR Epidemiology Group Manager, or designee prior to the release of the data. The Epidemiology Manager will review and approve (in writing) the response to the Branch Manager to validate that:
    - no confidential data are included in data files available for public use;
    - researchers requests for confidential data have been approved by the DSHS IRB and the DSHS Research Executive Steering Committee;
    - that the data set only includes the data requested by the researcher and approved by the IRB;

- the limited use data sets are not released without a signed confidentiality agreement from the researcher;
- all data sets used for application development and testing of software and/or technology infrastructure must be de-identified, unless otherwise permitted by DSHS information security standards;
- de-identified data sets prepared for test purposes must be reviewed and approved (in writing) by the TCR Epidemiology Group Manager, or designee, to ensure that the data has been properly de-identified; and,
- patient specific data may be exchanged with the original reporting facility or other cancer control agency as appropriate and permitted by law for the purposes of obtaining information necessary to complete a case record. These agencies and facilities must comply with the TCR confidentiality of information and non-disclosure policies and procedures.

The TCR shares non-patient specific data with those approved for such purposes or that support general information requests, however, there are many exclusions from this, primarily related to patient specific data. These include, but are not limited to the following:

- the TCR does not share patient specific data received from one reporting facility with any other reporting facility (Note: reporting facilities making this type of request should be advised and encouraged to work directly with the other reporting facility in order to meet their needs);
- TCR will not disclose social security numbers (SSNs) to requestors of cancer data (42 USC Section 405c(2)(C) (viii));
- when TCR staff conducts training and demonstrations of TCR software, reporting forms, or reports, staff must use fictitious, redacted, or de-identified information.
- de-identified data sets prepared for these uses must be reviewed by the Epidemiology Group Manager, or designee, to verify that the data has been properly de-identified. The manager or designee must document the following in writing:
    - the person designated to conduct the review;
    - the date the review was conducted;
    - that the file was properly de-identified by the person preparing the file; and

- that there was a secondary review of the data and the data request.

TCR staff must exercise extreme care and follow approved procedures and processes in sending confidential information. There are a few ways in which this data can be shared:

- Web Plus Server - The primary and preferred way to send out data to reporting facilities or other entities with approval to receive such data is via the Web Plus Server (also reference the "Web Plus Server Security" later in this document);
- Hand-delivery or hard copy;
- Fax

When sending out confidential data or information via Web Plus Server the TCR staff member must do the following **BEFORE** sending out the data:

- secure written authorization/approval to send out the data from the manager or their designee (primarily the team lead) ; (Note: the authorization/approval may be general by record types or specific to a single transmittal); and,
- verify that recipients have a Web Plus Use and Confidentially Statement and Web Plus User Form complete and on file with the TCR.

When sending confidential data or information out via hand-delivery or hard copy**,** TCR staff must:

- get written confirmation from the Branch Manager or designee approving the use of this method; and
- ensure that the policies and processes for transporting confidential information outside of the TCR offices as outlined under the section in this document related to "Physical Safeguards" are understood and followed.

When sending confidential data or information out via fax, staff must:

- get written confirmation from the Branch Manager or designee approving the use of this method;
- use only fax machines for this purpose when they are located in secure areas of TCR central and regional offices;
- verify or conduct, after receipt of the written approval to use a fax:
    - the name of the person receiving the information;

- that the person receiving the information has authority to receive the confidential information;
- the fax number with the person receiving the information;
- that the person receiving the information will be in the area of the receiving fax machine upon the fax being sent and/or that the receiving fax machine is in a secure location;
- that the recipient has been contacted immediately after the fax confirmation page prints to verify the receipt of the documents;
- remove the documents containing the confidential information immediately after the fax has been sent; and,
- print and retain the fax confirmation pages in accordance with TCR's Records Retention Schedule.

When receiving confidential information, the preferred method is via the Web Plus server. If a reporting entity or other entity **relates a compelling business reason why they cannot use the Web Plus server**, confidentially marked sealed double enveloped hand-delivered hard copies or faxing to a secure TCR is acceptable. CD's, diskettes, emails, mail, overnight delivery, etc. cannot be used to transmit data to the TCR. TCR staff should work closely with the reporting facility who will be sending confidential information to the TCR. TCR staff and/or entities sending information to the TCR should:

- encourage facilities or other entities to use the Web Plus Server to send data to the TCR;
- consult the TCR web page for instruction for using the Web Plus servers to send information to the TCR;
- consult with the TCR help desk (Systems Analyst) for assistance in getting a password or additional help in use the Web Plus Server;
- ensure the transmission of data hand-delivered to the TCR by hand-delivery and that a TCR staff member will be available to accept and secure the data and that the delivery will be during the TCR's normal business hours;
- ensure that when receiving confidential information by fax that arrangements are made before faxing the information to ensure that a TCR staff member will be available to receive and secure the incoming fax and that the fax will be during the TCR's normal business hours; and,
- use only fax and/or copy machines that are located in secure areas of the TCR central and regional offices.

When sending individual record level data sets, whether de-identified or not, the sets must be sent to the recipient via the Web Plus server.

TCR staff members, on rare occasion, may remotely access a facility's medical records for the purpose of abstracting or other business need. TCR staff member(s) and facilities granting remote access must comply with or conduct the following:

- access to the facility's electronic systems must be on the basis of least privilege with TCR staff members receiving only access to limited information and system resources that are necessary to conduct the work;
- ensure that access privileges comply with all applicable state and federal laws, including the Texas Medical Privacy Act and HIPAA;
- ensure that the facility has the capability to restrict TCR staff member access to only the medical records the staff member requires to conduct the work;
- limit the access for a defined time period that lets the staff member complete the work;
- ensure that access will be via a VPN (Virtual Private Network) or other secure means;
- receive written approval for access by the facility's Medical Records Director, Health Information Management Director, or other person authorized to provide approval (sent to the Branch Manager or other appropriate manager or designee);
- provide a written authorization by the Branch Manager or designee back to the facility approving the remote access;
- ensure that the TCR staff member with remote access has signed the applicable facility's confidentiality agreement and that the agreement is filed with TCR and recorded in the "Confidentiality Forms and Agreements" log; and,
- ensure that within 3 days of completing the work for which remote access was granted, or in the event that an employee leaves TCR, that a request is sent to the responsible facility official by the TCR staff member's manager requesting that access be terminated.

There are rare instances when it may be permissible to share PHI via the phone, however this should only be done when the the caller is known to the TCR staff member and/or can be verified if unknown. The exchange of PHI should be kept to the minimum necessary to respond to the request or need

for information. You must consult with your manager before sharing any level of PHI via the phone.

WEB PLUS SERVER SECURITY

Web Plus is the software used for securely transmitting/receiving cancer cases to the TCR. Web Plus is a web-based application provided by the Centers for Disease Control and Prevention (CDC) that also collects cancer data securely over the internet. More information about Web Plus can be found at the CDC website at http://www.cdc.gov/cancer/npcr/tools/registryplus/wp.htm.

To establish access to the TCR Web Plus server, each user organization must complete a "Web Plus Use and Confidentiality Statement" form found at https://www.dshs.texas.gov/tcr/webplus.aspx, sign the document, and email, mail, or fax it back to the TCR. Incomplete or unsigned forms will not be accepted. The TCR can grant, terminate, and refuse access to the Web Plus server at its sole discretion and at any time.

Once a user organization is approved to access the Web Plus server, individual users should complete and submit a "Web Plus User Information Form" found at https://www.dshs.texas.gov/tcr/webplus.aspx to the TCR. This information will aid in creating a Web Plus account. The "User Information " form should be completed by all account users and submitted back to the TCR by mail, email, or fax. Incomplete forms will not be accepted and the submitter notified.

It is the responsibility of the user organization with access to Web Plus to maintain the confidentiality of their account. The user organization must:

- designate two persons to be responsible for their facility's account; only these two people will be granted Web Plus server access privileges and only these two people may request password resets or account changes (please note – TCR's preference is that each person set up their own Web Plus account);
- verify the user organization's identifying number when contacting the TCR for Web Plus assistance (Note: each user organization has a number identifier assigned to them by the TCR, when they calling the TCR, this identifying number must be given by the designated user organization); and,
- report any changes to their Web Plus account to the TCR (this includes, but is not limited to, circumstances where a designated person is no longer with the user organization or a new representative for the user organization has been hired).

The TCR may allow more than two individuals from a user organization to access the Web Plus server if there is a valid business necessity, the exception is approved by the Branch Manager, and all other security requirements can be met and maintained.

Once all information has been collected from a user organization and its individual users, the TCR Systems Analyst will add that information to a secure and encrypted spreadsheet maintained on a secure server drive with limited password reset account access granted in Web Plus to Data Management staff members.

On occasion, user organizations will make requests for password resets. Requests for password resets will be processed using the following rules:

- user organization representative:
    - calls the TCR Help Desk requesting a password reset in the Web Plus server; and,
    - user organization representative states their name and identifying number.
- the TCR Help Desk then:
    - ask a confidential question that only the user organization representative will be able to answer (the information is based on the information completed on the form the organization submitted to the TCR);
    - verifies all information and if correct proceed to change the password in Web Plus; and,
    - calls back (or sends a secure email to) the user organization representative using the phone number provided on the "*User Information*" form and provides the updated password information

To optimally maintain the integrity and security of the Web Plus server, non-case submission files (i.e., non-NAACCR files) must be moved off of the server immediately following upload or download. Incoming files must be moved to a network drive when received and outgoing files shall be removed after receiving confirmation of retrieval by the recipient. Files must only be removed using Ax Crypt software. This is important both to keep file directories organized and for data security as most of these files contain confidential information. The System Analyst will monitor non-case submission files to ensure this policy is being enforced.

RETENTION OF REPORTS OF CANCER TO THE TCR

All original reports of cancer including copies of medical records submitted to the TCR will be retained for up to one year from date of receipt. All non-reportable reports of cancer will be purged from TCR databases no later than one year from date of receipt.

MAINTENACE AND DATA SECURITY OF LAPTOP COMPUTERS

General monthly maintenance will be performed on all laptop computers available for check-out as follows:

- each Regional office must designate one primary and one backup person to ensure maintenance of laptop computers in the regional office; maintenance of laptop computers will be performed by the Systems Analyst in the central office; and,
- laptops must be connected to the DSHS domain to launch and receive updates once a month.

Confidential information must be removed from laptop computers using the following process (note: the storage of confidential information on TCR laptops is now a rare occurrence):

- all laptop computers must be loaded with Ax Crypt software (Ax Crypt software is approved by DSHS IT security for proper shredding and deletion of secure files);
- after laptop computers have been loaded with any confidential information, the files containing confidential information must be removed on the first, but no later than the next business day after returning to the office by "shredding and deleting" using the Ax Crypt software; and,
- if the files containing confidential information are deleted without using shred and delete in Ax Crypt, the laptop computer must be wiped using DBan software and the laptop computer must be reimaged (Note: the TCR Systems Analyst and primary designee or backup person [regional office] is responsible for having the laptop computer reimaged by DSHS Central or Regional IT computer support).

The TCR Systems Analyst will provide training and serve as a resource to the Regional Office primary designees and backup persons on conducting monthly maintenance and proper use of Ax Crypt as needed.

ACCEPTABLE ENCRYPTION METHODS

All confidential information that is transported physically on laptop computers or transmitted electronically via Web Plus by TCR staff must be encrypted and password protected using the PGP encryption application(s) provided. The following policies also apply to encryption of data by entities outside of the TCR:

- all data files containing confidential information owned or provided by the TCR must be encrypted and password protected when being transmitted and at rest using either the PGP encryption application or other approved encryption software;
- files uploaded or downloaded via the Web Plus server are automatically encrypted in transit and at rest and should not be separately encrypted; and,
- any entity outside of the TCR transmitting or retaining TCR data files containing confidential information should consult with their Information Security Officer to ensure the software used meets NIST standards and can be decrypted by the TCR without installation of additional software.

INTERNET AND INTRANET SECURITY

Information and data transmitted via Intranets and the Internet are susceptible to inadvertent, unauthorized or illegal interception and use. Security precautions can be taken to minimize this possibility. Employees, contractors, volunteers and those visitors who will be allowed access to confidential information must abide by the following rules when electronically transmitting any confidential information:

- individuals with access to TCR's confidential information who are using emails or email attachments, including encrypted email and/or encrypted email attachments, are prohibited from transmitting confidential information using email to transmit confidential information (Note: The use of hyperlinks using DSHS/HHSC secure systems are permitted only when those individuals are TCR employees and when the files exist on the TCR secure network);
- when electronically transmitting confidential information via the Web Plus server the Web Plus server security policy and procedure must be followed (See "Web Plus Server Security" earlier in this policy);
- uploading or downloading confidential information to or from any Internet website may only be performed if the website includes as part of its controls 1) encryption/ decryption of data using an encryption key, 2) individual user passwords, and 3) use of a Secure Socket Layer (SSL), Secure HTTP (HTTPS), WinSock FTP (WS_FTP) or Secure FTP

(FTPS) protocol for transmitting data. The Branch Manager must approve any exceptions in writing.

TERMINATION OF ACCESS

Securing TCR data systems is a critical component of TCR operations. When an employee or contractor leaves the TCR and/or stops work with the TCR the manager or designee must follow procedure and processes to terminate access to computer, network, email, Internet, Registry Plus application and the TCR Web Plus Server on the date of separation.

CONTRACTORS

Occasionally, the TCR will hire contractors to help in TCR's work. Contractors and/or those involved in securing the contract are required to:

- understand and follow all physical, electronic, data exchange, and security requirements of the TCR;
- report immediately to the Branch Manager any incident that may compromise TCR data on the same day of the possible event;
- include in any TCR Request for Proposal (RFP), Request for Offer (RFO), Invitation for Bid (IFB), etc. a copy of the TCR Confidential Information Security Policy;
- comply with and sign the TCR Confidentiality and Non-Disclosure Agreement before the work begins;
- comply with HHS policy and sign the HHS Acceptable Use Agreement (AUA)
- ensure (except for when it is an individual contracting with the TCR) that each contractor has in place an information security plan and provide it to the TCR for review and approval before the work begins;
- ensure (in the case of individuals contracting with the TCR) have an information security plan that is approved by the TCR and/or that they adopt the TCR Confidential Information Security Policy;
- ensure that any contractor or entity not receiving approval for their plan or adoption of the TCR Confidential Information Security Policy does not obtain access;
- ensure that all contractors or contractor employees receive, read, and understand the TCR Confidential Information Security Policy prior to work beginning;
- ensure that the laptop or personal computer used for TCR work are secure, have, and keep activated a DSHS approved anti-virus

software, and kept current with the latest appropriate security updates;

- ensure that laptops used by the contractor to perform TCR work not be used for any activity other than the TCR's contracted work over the course of the contract term; and,
- ensure that when the contracted work/contract is over that the contractor provides a written verification that they have removed all TCR confidential information from the laptop or other device using TCR approved procedures.

CONFIDENTIAL INFORMATION INCIDENT REPORT PROCEDURES AND PROTOCOLS

TCR staff must be mindful that if they suspect or know of a potential confidential information incident they must report that to their supervising manager and/or the Branch Manager.

On occasion, a potential or actual incident may occur that potentially compromises or discloses TCR data. These include, but are not limited to:

- unintended mistakes that cause accidental disclosure;
- abuse of access privileges;
- accessing information for profit;
- unauthorized physical intruders in TCR offices and facilities; and,
- attempts to access information to damage surveillance systems and disrupt operations.

TCR staff have an important responsibility to assure that TCR confidential information remains secure and confidential. Staff can do this in many ways that include, but are not limited to:

- being and remaining aware of their surroundings and activities;
- reporting any possible incidences to their manager if they are aware of, observe, or suspect an activity that potentially compromises TCR confidential information or data;
- maintain written documentation by the approving manger that the activity is approved;
- report immediately any activity that has not been approved; and
- handle (in consultation with their manager) and report any possible breaches of TCR confidential information quickly.

When a report of a possible incident is received by the appropriate manager, or their designee, that person must:

- start an immediate response focused on the information and/or the work area that helps to mitigate the potential for risk or exposure. Depending on the severity of the issue, these steps can include, but are not limited to:
    - Shutting and locking door (keeping appropriate safety measures in mind) and file cabinets;
    - report unauthorized person in the building or TCR work space to either security personnel for that building and/or the employee's manager or designee;
    - attempt to and/or retrieve the unauthorized information or data if it can be done safely;
    - ALWAYS notify IMMEDIATELY the staff's manager and/or the CBO Manager, or Branch Manager by telephone with known facts and the immediate mitigation steps;
- limit hard copy file and/or computer access for any person(s) who caused or was involved in the incident until the incident has been reported, mitigated, and reviewed;
- reassign the TCR staff member or contractor immediately to other work and/or with direction by the Branch Manager, send that individual home;
- suspend, if a contractor is involved, the contractor until the incident has been reported, mitigated, and reviewed; and,
- call, only in consultation with the appropriate manager, law enforcement if criminal violations are suspected. These include but are not limited to:
    - theft;
    - tampering with a governmental record – intentionally destroying, concealing, removing or otherwise impairing the truth, legibility, or availability of a governmental record;
    - criminal mischief – intentionally or knowingly damaging or destroying property of another or tampering with property of an owner and causing financial loss or substantial inconvenience to the owner or other person; or
    - breach of computer security – knowingly accessing a computer, computer network, or computer system without the effective consent of the owner of that system.

When a suspected incident occurs, the following steps must also be taken by the staff member, their manager or the Branch Manager and/or their designee, within one business day after the incident occurs and/or is discovered:

- consult the DSHS Privacy Office Privacy Incident (Breach Reporting) page for the latest DSHS direction (http://online.dshs.internal/cpea/Privacy-Incident-Reporting.aspx) and complete and submit to the Branch and/or Core Business Operations Manager the DSHS Privacy Incident Reporting Form found on that page.
- include in the report a detailed description of what occurred, when it occurred, who was involved, when and to whom it was reported, events leading up to what occurred, and steps taken to mitigate the immediate impact by both the staff member and their manager;
- The Branch Manager must:
    - report to the DSHS Privacy officer, the DSHS privacy attorney, the Environmental Epidemiology and Disease Registries' Section Director, any incident that involved protected health information;
    - notify, upon confirmation of the incident and within timeframes established by applicable statutes, rules, guidelines, and protocols, the affected medical provider and/or reporting entity who originally submitted the TCR about the incident and steps taken to mitigate the issue;
    - ensure that before sending out the notice to the impacted entity that the draft notification has been reviewed and approved in accordance with DSHS policy and procedure;
    - notify, if the confidential information incident involves state owned computer equipment, networks, or data storage devices, the DSHS Computer Incident Response Team (CIRT) in accordance with current DSHS Information Security Standards and Guidelines and Computer Incident Response Plan
    - ensure that all TCR staff cooperate with the CIRT; and,
    - appoint a TCR security team (including at least the employee's supervising manager, the CBO manager and others designated by the Branch Manager) to examine any suspected, unauthorized or reported confidential information incident (note: DSHS IT staff will be consulted or participate on the security team dependent on the type and nature of the possible incident.

A thorough review of the incident is important not only to responding to and mitigating the issue immediately, but to implement steps that will prevent future similar incidents and provide opportunities to remind staff , potentially modify protocols, and/or provide additional training.

The TCR Security Team will:

- determine the validity of a suspected or reported confidential information incident;
- complete and sign, if the incident is found to be invalid, the "Description and Sequence of Events, Findings, and Recommendations" section of the TCR Confidential Information Incident Report form and submit the form to the Branch Manager.
- do, upon confirmation of an incident, steps that include, but are not limited to:
    - reviewing the accountability, management controls, electronic controls, physical security controls and penalties relevant to the situation to identify gaps and weaknesses and opportunities to prevent future occurrences;
    - recommend and upon approval of the Branch Manager, implement steps to address the current incident and/or implement processes and/or practices to avoid or minimize future incidents;
    - make, in consultation with the TCR Branch Manager, recommendations or actions that include, but are not limited to:
        - informing appropriate parties and offices that include the Office of General Counsel's Privacy Attorney, the Section Director of the Environmental Epidemiology and Disease Registries Section, the Associate Commissioner for Disease Control and Prevention, the Deputy Commissioner and/or Commissioner, The DSHS Information Security Officer, the DSHS Privacy Officer, and other senior DSHS managers or offices;
        - refer the matter to the HHS Office of Inspector General for further review and/or investigation;
        - refer, to the DSHS Office of General Counsel's Privacy Attorney and the DSHS Human Resources representative, for any potential legal action against a staff member, individual or contractor found to be responsible for releasing or accepting confidential information;

        - conduct, as appropriate, a risk analysis or penetration testing;
        - create, if necessary, new, supplemental or revised policies, procedures, trainings, or practices to address any gaps or opportunities for improvements identified;
        - refer the matter, if needed, to the contractor whose staff caused the incident and require that they follow up on the steps (in writing to the TCR) they take to resolve the complaint; and
        - apply, if appropriate, sanctions to a contractor that does not quickly act to review and address the matter;
    - Complete and sign, at the conclusion of the review, the "Description and Sequence of Events, Findings, and Recommendations" section of the TCR form and submit the completed the form to the Branch Manager. Include with the report, any documentation that was reviewed and/or created as a result of the review.
    - The Branch Manager; upon receipt of the incident report will:
        - concur with the findings of the security team;
        - direct that additional review and/or documentation is needed;
        - note additional exceptions or additions to the findings and recommendation, sign the form, give the team the approval to implement the recommendations, and send the report to others, as appropriate to the incident; and
        - send the final form, to the DSHS CIRT or other required offices, if the incident involved state owned computer equipment, networks, or data storage devices for their further use and consideration.
        - send, as appropriate and after review and approval to send, a communication to the medical provider and/or health care facility regarding follow-up taken and findings.

All media contacts related to a confidential information incident must be referred to the DSHS Center for Consumer and External Affairs (CCEA), Communications Unit with a copy to the Branch Manager.

All TCR forms and documentation related to security incidents must be stored in TCR central and/or computer files after resolution and reviewed in accordance with The TCR Record Retention Schedule.

SUMMARY

All TCR staff and those entrusted with TCR data, have the responsibility to maintain and work with confidential information that meets the TCR standards, policies and guidelines.

TCR staff must be diligent in:

- reporting suspected or known incidents to their manager or that person's designee:
- understanding, adhering to and implementing TCR standards, policies and guidelines;
- being aware; and ,
- maintaining appropriate security measures, within the scope of their own work that meets the requirements, and protects the confidential information with which we are entrusted.

No policy, guideline or requirement can address every nuance of the issue or topic it covers. Each staff member must ask questions of their manager, or that person's designee if they have questions, don't understand something, or have recommendations or suggestions. Finally, each staff member must also exercise a certain amount of common sense when reporting issues, responding to the recommendations, and implementing remedial activities.

When in doubt, consult with your manager.

Our customers, and the persons whose data we are entrusted with expect that diligence and effort.

APPENDIX 1 – CONFIDENTIALITY AGREEMENT

(Next Page)

TEXAS DEPARTMENT OF STATE HEALTH SERVICES
CANCER EPIDEMIOLOGY AND SURVEILLANCE BRANCH
CONFIDENTIALITY and NON-DISCLOSURE AGREEMENT

The purpose of the confidentiality policy for the Texas Cancer Registry (TCR) is to protect the privacy of individual patients, physicians and institutions reporting cancer cases; to provide public assurance that the data will not be abused; and to abide by confidentiality-protecting legislation or administrative rules that may apply.

The TCR receives and collects protected health information from facilities required to report incidences of certain tumors and cancers under Health and Safety Code, Chapter 82. Information collected by the TCR is confidential by statute and is not subject to disclosure by the Texas Department of State Health Services (DSHS) or any person acting on behalf of the department, except as authorized by Health and Safety Code, Chapter 82. The undersigned person is authorized by the TCR to receive and use protected health information on behalf of the TCR.

Each person who receives, reviews or evaluates information made confidential by state or federal law is required to sign the following Confidentiality and Non-Disclosure Statement:

My name is _____, my position title is _____ and I am employed by or working at _____. In the course of my duties I will receive, review and/or evaluate protected health information, which also may include extracting and entering reportable data on behalf of the TCR, for the purpose of assisting the DSHS in complying with the requirements of Health and Safety Code, Chapter 82.

I understand that this protected health information is confidential and not subject to disclosure by DSHS, or me except as authorized by Health and Safety Code, Chapter 82.

I understand that the TCR is required to protect information collected and received from further disclosure and that even an inadvertent disclosure could result in serious loss, destruction or unauthorized disclosure of confidential information received and collected by the TCR.

If I am an employee, temporary employee or contractor of the TCR, I understand that failure to comply with the confidentiality policies may result in firm disciplinary action up to and including termination of my employment or contract.

I understand that any disclosure by me could result in serious civil and criminal legal action being taken against me, as provided by Texas Government Code, Chapter 552. Unauthorized disclosure could also subject me to civil and criminal penalties under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) to the extent protected health information is used or disclosed in violation of the Privacy Standards at 45 C.F.R, Parts 160 and 164; under 38 U.S.C. Sec. 5701 (Veterans' Records); and under other state or federal civil and criminal laws.

I understand that this agreement remains in effect in perpetuity after I terminate my employment or working relationship with the TCR.

I agree that I will not disclose or use any of the information made available to me by the TCR, except as authorized by the DSHS and in accordance with DSHS policies and procedures. I agree that I will not reproduce in any way, including taking notes or producing handwritten memos, the content or the uses of the confidential information provided to me by the TCR. If I take notes or memos for my own use, I will give them and any copy I make of them to the TCR at the termination of my employment or working relationship with the TCR.

I agree to cooperate in any investigation regarding a breach of confidential information conducted by the TCR, DSHS, its affiliated investigative units or any law enforcement agency.

_____ **(INITIAL HERE)** I have read, understand and agree to abide by the Texas Cancer Registry Policy and Procedure Regarding Confidential Information. I further agree to respect and preserve the confidentiality of TCR information in protecting the privacy of individual patients, physicians and of institutions reporting cancer cases.

_____	_____
Signature	Approving Official
_____	_____
Title	Date Signed

APPENDIX 2 – LIMITED-USE DATA REQUEST FORM

(Next Page)

TEXAS Health and Human Services | Texas Department of State Health Services

Texas Cancer Registry
Limited-Use Data Request Form

Background: Protecting patient confidentiality and other protected health information (PHI) is paramount to the Texas Cancer Registry (TCR), Cancer Epidemiology and Surveillance Branch, Texas Department of State Health Services (DSHS) and required by state law and rule (Health and Safety Code, §82.009; Texas Administrative Code, Title 25, Part 1, Chapter 91, Subchapter A). All personal identifiers [name, date of birth (excluding year), social security number, address (excluding county), census tract, block, latitude/longitude, reporting health care facility, pathology laboratory, or health care practitioner, telephone number, and date of diagnosis] must be removed from data before release, unless prior approval is obtained from the DSHS IRB. Limited Use data, or any de-identified data provided in electronic format, does include certain demographic information, such as sex and race, for research purposes. The TCR requires that all research results be presented/published in a manner that ensures that no individual can be identified. In addition, there must be no attempt to identify individuals either from any computer file, or by linking with another source of data containing patient identifiers.

Instructions: Before the TCR can provide a limited-use dataset, please complete and return this form to the TCR at CancerData@dshs.texas.gov or fax to 512-776-7681, Attn: TCR Epidemiology Group.

1. **Name, address, title, agency/institution of person requesting access to data:**

2. **Name, degree(s), title, mailing address, email address, and phone number of person who will direct the project or study:**

3. **Summary/synopsis of the project or study:**

4. **Is the project or study funded?** ☐ Yes ☐ No

   If yes, please list the funding entity:

In order for the TCR to provide a limited-use or another version of data to you, it is necessary that you agree to the following provisions.

1. You will not use nor permit others to use data in any way other than for statistical reporting and analysis for research purposes. If you discover a breach of confidential information, you must notify the TCR without delay (Maria Vega, Core Business Operations Manager, 512-776-3603 or Melanie Williams, Branch Manager, 512-776-3633), describing the known facts of the incident, and the immediate mitigation steps taken, so that we can begin the process of mitigating the effect of the breach and prevent any additional loss of data as soon as possible.

2. You will not present/publish data in which any individual can be identified. You will not publish any statistics on a single individual including any information generated on an individual case by the case listing session of SEER*Stat, or any other analysis software. In addition, publication of small cell sizes should be avoided.

3. You will not attempt to link nor permit others to link the data with individually identified records in another database.

4. You will not attempt to learn the identity of any person whose cancer data is contained in the supplied file(s).

5. If the identity of any person is discovered inadvertently:
    a. No use will be made of this knowledge;
    b. TCR Branch Manager, Melanie Williams, Ph.D., be notified of the incident immediately by calling 512-776-3633 and/or emailing Melanie.Williams@dshs.texas.gov; and
    c. No one else will be informed of the discovered identity.

6. You will not release nor permit others to release the data in full or in part to any person except with the written approval of the TCR. In particular, all members of the research team who have access to the data must have signed data-use agreements.

7. You will use appropriate safeguards to prevent use or disclosure of the information other than as provided for by this data-use agreement. If accessing the data from a centralized location on a time-sharing computer or LAN with SEER*Stat or another statistical package, you will not share your logon name and password with any other individuals. You will also not allow any other individuals to use your computer account after you have logged on with your logon name and password.

8. The source of information should be cited in all publications. The appropriate data citation is associated with the specific data file used. In addition, the TCR requests that you include the following statement of acknowledgement in the text or frontispiece of the presentation, report, or publication: "Cancer incidence data have been provided by the Texas Cancer Registry, Cancer Epidemiology and Surveillance Branch, Texas Department of State Health Services, 1100 West 49th Street, Austin, TX 78756."

My signature indicates that I agree to comply with the above stated provisions.

_____	_____
Signature	Date
_____	_____
Printed Name	Phone Number
_____	
Title	

Please indicated format of requested data set:

☐ SEER*Stat Cancer Incidence data set

☐ SAS Cancer Incidence data set

Name of Person Responsible:

Data Request Number: _____ (Internal Use Only)

APPENDIX 3 – WEB PLUS ACCOUNT REGISTRATION

Online form available at:
https://www.surveymonkey.com/s/TCRWebPlusRegistration

APPENDIX 4 – WEB PLUS USE AND CONFIDENTIALITY STATEMENT

(Next Page)

Web Plus Use and Confidentiality Statement

Texas Department of State Health Services | Cancer Epidemiology and Surveillance Branch

This Web Plus use and Confidentiality Statement, by and between the ***Texas Department of State Health Services, Cancer Epidemiology and Surveillance Branch, Texas Cancer Registry*** (CESB, hereinafter) and _____ (User Organization, hereinafter) made and entered into on _____ (date) concerning access to and use of Web Plus.

CESB agrees to:

a. Provide access to and technical assistance for Web Plus, but will not support other software or hardware defects or problems that are unrelated to Web Plus.

b. Provide a help desk for assistance with questions and technical support. The help desk is available Monday through Friday from 8:00 am to 5:00 pm CST by calling (512) 776-3617, (800) 252-8059, or by email at pam.jatzlau@dshs.state.tx.us.

c. Maintain Texas Cancer Registry (TCR) data in compliance with Texas Health and Safety Code Chapter 82, Texas Administrative Code (25 TAC 91) and the TCR Confidential Information Security Policy.

User Organization agrees to:

a. Keep a list of their organization's authorized Web Plus users, and notify the CESB office at (512) 776-3617, (800) 252-8059, or via email at pam.jatzlau@dshs.state.tx.us of any change of User Organization personnel accessing Web Plus.

b. Review and instruct all User Organization personnel that will have access to Web Plus on the confidentiality of TCR data pursuant to Texas Health and Safety Code Chapter 82, Texas Administrative Code (25 TAC 91) and the TCR Confidential Information Security Policy.

c. Ensure that Web Plus and any confidential information transmitted to or from the Web Plus application server is not used in a manner other than expressed in the Texas Health and Safety Code Chapter 82, Texas Administrative Code (25 TAC 91) and the TCR Confidential Information Security Policy.

d. Lose Web Plus user rights if abuse of privileges or TCR data is suspected or confirmed.

Use and Confidentiality Statement:

By signing this use and confidentiality statement, I certify that I have read this use and confidentiality statement and agree to comply with the following:

a. I will distribute copies of this use and confidentiality statement to all assigned personnel accessing Web Plus.

b. I agree to be held responsible for my assigned personnel's actions regarding information transmitted to or from Web Plus.

c. Protected health information transmitted to or from Web Plus is confidential and must be used only for the purpose it is collected pursuant to Texas Health and Safety Code Chapter 82, Texas Administrative Code (25 TAC 91) and the TCR Confidential Information Security Policy.

d. Unauthorized disclosure of personally identifiable information is prohibited.

e. Any unauthorized disclosure of TCR information may result in my losing the ability to access Web Plus.

f. I agree NOT to share the Web Plus User ID, password, or URL with any unauthorized users.

g. I verify that I am an authorized Web Plus user and I will use the security level assigned by the CESB.

h. I have read and agree to the terms on this Web Plus Use and Confidentiality Statement.

Signatures: (The Access Administrator and Primary User Must Sign)

Name of User Organization: _____

_____	_____	_____
Print Name (Primary User)	Signature	Date
_____	_____	_____
Print Name (Administrator)	Signature	Date

Web Plus Account Security Question: (Please choose **one** of the following to answer)

a. What is the name of your favorite pet? _____

b. What is your father's middle name? _____

c. What is the name of your birthplace city? _____

d. What is your favorite color? _____

Note: When requesting a password reset for your Web Plus account, it is required that you know the correct answer to the security question chosen.

Upon completion, please scan and email, fax, or mail your signed form to the CESB (*see contact information below*). After the CESB receives your form, staff will contact you within two business days to complete the setup of your Web Plus account.

Texas Department of State Health Services
Cancer Epidemiology and Surveillance Branch MC 1928
P.O. Box 149347
Austin, Texas 78714-9347
Fax: (512) 776-7681
Email: pam.jatzlau@dshs.state.tx.us

Thank you for completing this form in its entirety.

APPENDIX 5 – DSHS PRIVACY INCIDENT REPORTING FORM

Available online:

http://online.dshs.internal/WorkArea/linkit.aspx?LinkIdentifier=id&ItemID=45881