TCRN STANDARD OPERATING PROCEDURE	
TITLE: Incident Reporting	**NUMBER: SOP-7 Version: 5**
PREPARED BY: **Julia Corrigan, University of Pittsburgh**	**APPROVED BY:** **TCRN Executive Committee**
DATE WRITTEN: **April 16, 2015**	**ISSUE DATE:** **July 1, 2015**

1.0 PURPOSE:

The TIES Cancer Research Network (TCRN) provides access to large cohorts of data and samples. This policy describes incidents that may arise in TCRN and how member institutions must report and respond to them.

2.0 REVISION HISTORY:

Date	Rev. No.	Modification
4/16/15	1	Drafted by Julia Corrigan
4/21/15	2	Modified by Julia Corrigan
5/14/15	3	Modified by Julia Corrigan
5/15/15	4	Minor modifications by Liz Legowski and Julia Corrigan
6/3/15	5	Modified by Julia Corrigan

3.0 PERSONS AFFECTED:

The TIES Regulatory Administrators, TIES IT Administrators, TCRN Quality Assurance personnel, and TCRN Users are affected by this policy.

4.0 POLICY:

It is the policy of the TCRN that each TCRN institution will respond to and report incidents, which are described below. TCRN users and personnel must take the actions described below to address incidents. TIES Regulatory Administrators are responsible for managing all incidents, which includes filling out incident forms and overseeing incident handling.

The Regulatory Administrator must report incidents to other TCRN member institutions if indicated below. Incidents should be reported to the Policies and Procedures Subcommittee unless otherwise specified. Additionally, member institution must develop and follow local incident reporting policies.

5.0 DEFINITIONS:

TIES – The Text Information Extraction System is a computer-based system that establishes a repository of natural language processing (NLP) coded, de-identified pathology reports for the purpose of identifying cohorts and cases associated with formalin fixed paraffin embedded materials, frozen tissues, or other research resources.

TCRN – The TIES Cancer Research Network represents all member institutions that have signed the TCRN Network Agreement, with the intent of supporting collaboration (data, tissue, or data and tissue) across institutions that have deployed the TIES system.

TCRN User – A TCRN user is a TIES user who has one or more TIES protocols allowing use of de-identified from another TCRN institution (in addition to their own).

Valid User – A user who has legitimate access to TIES given local policies, and who has been deemed an Authorized User by one or more TCRN sites.

TIES Regulatory Administrator – The Regulatory Administrator approves studies, drafts regulations, and communicates with other TCRN institutions through the TCRN Policies and Procedures Subcommittee.

TIES IT Administrator – The IT Administrator verifies eligibility of local users and creates user accounts and studies.

TCRN Quality Assurance (QA) Manager – The QA Manager is responsible for conducting quality assurance and maintaining acceptable de-identification standards.

Approved Use – Describes range of activities approved by a given organization for a TCRN user as described in the TCRN Network Agreement, IRB protocol (if applicable), and Materials Transfer Agreement (if applicable).

TIES Protocol – Within TIES, the TIES protocol describes the research being conducted, one PI, and one or more investigators conducting the research. Each TIES protocol is associated with an honest broker. Searching in TIES requires that the user specify which protocol they are conducting their search under.

6.0 RESPONSIBILITIES:

The **TIES Regulatory Administrator** will manage incidents, report incidents to the TCRN, and draft local incident policies.

The **TIES IT Administrator** will change user permissions, put accounts on hold, or terminate accounts of users who fail to follow TCRN policies.

The **TCRN Quality Assurance (QA) Manager** will take action when de-identification failures occur.

TCRN Users will notify TIES administrators if they are assigned to incorrect user roles or studies, and will report suspected unauthorized use of their accounts.

TCRN INCIDENT TYPES AND PROCEDURES:

1. **Query Audit Inconsistency Found**: The **Quality Assurance (QA) Manager**, during periodic audits of user searches, will identify if users are searching for cases that are outside of their **approved use**. This policy is in compliance with the **Auditing of TCRN Users and Searches** Standard Operating Procedure. The following steps will be taken based on user infractions:

    A. The **QA Manager** will contact the TCRN user and the **Regulatory Administrator** at the user's institution.
    B. The **Regulatory Administrator** will take one or both of the following actions:
        a. Educate the user on proper, approved use of TCRN if they do not realize they are searching outside of approved guidelines.
        b. Instruct the user to request amendments to their current TCRN study or to request a new TCRN study if they need to access further data for their research.
    C. If the TCRN user does not comply, the **Regulatory Administrator** will report noncompliance to the **IT Administrator**.
    D. The **IT Administrator** will terminate access to the TCRN study.
    E. The **Regulatory Administrator** will report the incident to the TCRN within 5 business days.
    F. All TIES personnel will follow the local incident reporting policy. Any additional local policies apply to the user.

2. **System Password Shared:** The **QA Manager** will identify or the **TCRN User** will report that an account password has been shared. The following steps will be taken based on user infractions:

    A. The **QA Manager** or **TCRN User** will notify the **Regulatory Administrator** and **IT Administrator**.
    B. The **IT Administrator** will place the user account on hold.
    C. The **Regulatory Administrator** will report the incident to the TCRN within 5 business days.
    D. All TIES personnel will follow the local incident reporting policy. Any additional local policies apply to the user.

3. **System Accessed by Invalid User:** The **QA Manager** will identify that their TIES node has been accessed by an invalid user. This policy is in compliance with the **Auditing of TCRN Users and Searches** Standard Operating Procedure. The following steps will be taken based on user infractions:

    A. The local **IT Administrator** will terminate accounts of users who are no longer employees at the institution.
    B. The **IT Administrator** will put a hold on the user's account if IRB approvals and MTA approvals (if applicable) are no longer valid.

C. The **Regulatory Administrator** will report the incident to the TCRN within 5 business days.
D. All TIES personnel will follow the local incident reporting policy. Any additional local policies apply to the user.

4. **Incorrect Role Assigned to User**: The **IT Administrator or Regulatory Administrator** will identify or the **TCRN User** will report that the incorrect role or access level has been assigned to the user. The following steps will be taken:

    A. The **IT Administrator** will place the user account on hold.
    B. The **IT Administrator** will reset the user account with the correct role.
    C. The **Regulatory Administrator** will report the incident to the TCRN in certain circumstances:
        a. If the user was given access to the incorrect user role (particularly honest broker access), report incident to the TCRN.
        b. If the incident is identified before access is granted, the incident does not need to be reported to the TCRN.
        c. Reports to the TCRN should be made within 5 business days.
    D. All TIES personnel will follow the local incident reporting policy. Any additional local policies apply to the user.

5. **Incorrect User Assigned to Study**: The **IT or Regulatory Administrator** will identify or the **TCRN User** will report that the user was not assigned to the appropriate study. The following steps will be taken:

    A. The **IT Administrator** will revoke the user's access to the incorrect study.
    B. The **IT Administrator** will reassign the user to the correct study.
    C. The **Regulatory Administrator** will report the incident to the TCRN in certain circumstances:
        a. If the user was given access to TCRN study, report to the TCRN.
        b. If the incident is identified before access is granted to the user, or if the user is given access to a local study only, the incident does not need to be reported to the TCRN.
        c. Reports to the TCRN should be made within 5 business days.
    D. All TIES personnel will follow the local incident reporting policy. Any additional local policies apply to the user.

6. **System Breach**: **Network Security** or the **QA Manager** will identify that the TIES node has been breached. The following steps will be taken:

    A. **Network Security** will identify the problem and shut down the Node.
        a. If they do not, the **IT Administrator** will immediately get in touch with local IT department and shut down the TIES node.
    B. The **Regulatory Administrator** will notify the TCRN member institutions of the breach within 24 hours.
    C. The **Regulatory Administrator** will report information on the breach as soon as possible.

    a. They must indicate if the problem happened on the server or if it was specific to the TIES system.
D. All TIES personnel will follow the local incident reporting policy. Any additional local policies apply.
E. Node will rejoin the TCRN when Network Security and TCRN approve it.

7. **De-Identification Failure**:

7a: System-wide de-identification failure: The **QA Manager** will identify that there is a system-wide de-identification problem, which may be indicated by a rapid increase in quarantined reports. The following steps will be taken:

A. The **QA Manager** will report the incident to the **Regulatory Administrator**.
B. The **IT Administrator** will immediately shut down the TIES node.
C. The **Regulatory Administrator** will report the de-identification failure within 24 hours; they will report to TCRN member institutions via the Executive Committee.
D. Adverse event reporting will be required in the case of significant Protected Heath Information (PHI) leaks (e.g. patient's name).
E. All TIES personnel will follow the local incident reporting policy. Any additional local policies apply.

7b: Reports quarantined by users: This policy is in compliance with the **Validation of De-Identification Quality** Standard Operating Procedure.

A. **TCRN Users** will quarantine any reports that contain any Protected Health Information (PHI).
B. The **Regulatory Administrator** will report the incident to the TCRN within 5 business days.
C. The **QA Manager** will review the quarantined report and follow the following procedures:
    a. The **QA Manager** will manually reprocess quarantined documents to remove PHI and ensure they are properly de-identified.
    b. If the mistake is part of a larger PHI failure, the **QA Manager** will work with the de-ID vendor to identify the issue.
D. All TIES personnel will follow the local incident reporting policy. Any additional local policies apply.

8. **Attempt to Re-Identify a Patient**: The **QA Manager**, during periodic audits of user searches, will identify if a user may be attempting to re-identify a patient by searching for PHI. This policy is in compliance with the **Auditing of TCRN Users and Searches** Standard Operating Procedure. The following steps will be taken if re-identification is suspected:

A. The **IT Administrator** will disable the user's access to all TCRN studies.
B. The **Regulatory Administrator** will report the incident to the TCRN within 24 hours.
C. The **Regulatory Administrator** will talk to their institutional Privacy Officer.
D. The **Regulatory Administrator** and/or institutional Privacy Officer will speak with the user to determine whether the user was trying to re-identify a patient.

a. If the user was attempting to re-identify a patient, the **IT Administrator** will terminate the user account and the user will be referred to the institutional Privacy Officer.

E. All TIES personnel will follow the local incident reporting policy. Any additional local policies apply to the user.

7.0 APPENDICES:

TCRN Incident Report

Instructions: The TIES Regulatory Administrator must document all known information regarding the incident involving the TCRN. This information must be reported to the specified parties within the given timeframe.

Reporting Center: Click here to enter text.
Submitted By: Click here to enter text.
Date Submitted: Click here to enter text.

Information on Incident

Incident type:

☐ Query Audit Inconsistency Found
☐ System Password Shared
☐ System Accessed by Invalid User
☐ Incorrect Role Assigned to User
☐ Incorrect User Assigned to Study
☐ System Breach
☐ De-Identification Failure
☐ System-Wide De-Identification Failure
☐ Reports Quarantined by Users
☐ Attempt to Re-Identify a Patient

Date of Incident Occurrence: Click here to enter text.
Date Incident Discovered: Click here to enter text.
Incident Identified By: Click here to enter text.
Persons Involved: Click here to enter text.
Incident Description: Click here to enter text.
Steps Taken: Click here to enter text.

Refer to the **TCRN Incident Reporting Standard Operating Procedure** for required steps.

REFERENCES:

None