Cancer Trials Support Unit Security Overview

1. Introduction

The Cancer Trials Support Unit (CTSU), run by Westat, is a service of the National Cancer Institute (NCI) designed to facilitate access to NCI-funded clinical trials for qualified clinical sites and to support the management and conduct of those clinical trials. CTSU provides access to a wide range of information and support services for qualified investigators and research staff.

1.1 Purpose

This document provides an overview of the security policies and practices for the CTSU Enterprise System (CTSU-ESYS) applications and Information Technology (IT) systems. This document will be provided (upon request) to clinical site Institutional Review Boards (IRBs) or Ethics Review Boards (ERBs), to fulfill system security requirements, and for reference purposes. Westat does not enter into individual business agreements with clinical sites, nor can it complete local IRB/ERB applications on behalf of the clinical sites.

1.2 CTSU Applications

The CTSU-ESYS is a suite of integrated databases, applications, websites, and capabilities that support the CTSU activities and operations. These activities range from protocol development support, regulatory document processing, patient enrollment, data collection and quality assurance, data distribution, education, training, and CTSU Helpdesk support services. The main applications that comprise the CTSU-ESYS are the Regulatory Support System (RSS), CTSU Website, CTSU Enterprise Web Services (CEWS), Oncology Patient Enrollment Network (OPEN), Regulatory Data Transfer System (RDTS), CTSU Enterprise Transaction Engine for Rave (CENTER), Clinical Data Image Management System (CDIMS), Regulatory Image Management Systems (RIMS), Source Document Portal (SDP), Data Quality Portal (DQP), Site Audit Portal (SAP), Delegation of Tasks Log (DTL), Medidata Rave, and iMedidata. Medidata Rave and iMedidata are hosted applications.

2. Security Policies and Procedures

Security policies and practices for CTSU applications have been documented in the CTSU Systems Security Plan (SSP). These are based on the “Westat Information Systems Security Policies and Practices” (WISSP), as guided by the National Institute of Standards and Technology (NIST) Special Publication 800-37 Rev 1, "Guide for Applying the Risk Management Framework to Federal Information Systems" and compliance with the Federal Information Security Management Act (FISMA). The SSP is reviewed by senior CTSU staff and is updated and submitted to the NCI Project Officer at NCI on an annual basis. The WISSP is reviewed at least annually by the Westat Corporate Information Security Officer (CISO) and other senior management.

The objective of corporate and CTSU specific policies and plans is to protect systems and data from a wide range of threats that could affect the confidentiality, integrity or availability of data, and to comply with the various legislative and contractual requirements of Westat clients.

CTSU security policies and best practices are based on the Westat security policies and best practices found in the WISSP (available upon request) and guidelines that are specified in the National Institute of Standards and Technology (NIST) Special Publication 800-18, "Guide for Developing Security Plans for Information Technology Systems"; the International Standards Organization (ISO) standard 17799:2000, "Information Technology – Code of Practice for Information Security Management;" and relevant client- or agency-specific standards and guidelines.

Please refer to WISSP for detailed information on:

- Facility and computer security
- Data security
- Network and data communications security
- Personnel security
- Disaster recovery
- User assistance and incident reporting

CTSU specific security controls are discussed in the following subsections.

2.1 Facility and Computer Security

2.1.1 Two Factor Authentication

CTSU adds a second layer to security to all administrators, developers, and Westat internal users that have access to production data or digitized documents. This Multifactor Authentication (MFA) provides a significant security enhancement when authenticating users. The second factor of authentication is integrated using Duo Mobile, more information is available at https://www.duosecurity.com/static/pdf/Duo-Security-Product-Overview.pdf.

2.2 Data Security

2.2.1 Clinical Site User Access to Applications

Users logging into CTSU applications are authenticated by the Cancer Therapy Evaluation Program Identity and Access Management (CTEP-IAM) application, which is a National Institute of Health (NIH) sanctioned identity provider that is hosted by Cancer Therapy Evaluation Program (CTEP). The CTEP-IAM login credentials meet NIH requirements. CTSU provides authorizations only, limiting authenticated users access to applications and parts of applications as determined by their affiliation to clinical sites. Access to Personally Identifiable Information (PII) is controlled at the user level.

CTEP-IAM passwords expire at set intervals. Applications are designed to lockout users after three failed login attempts. Applications log out users after 60 minutes of inactivity. User activity is logged, and an audit trail of data changes is preserved.

2.3 Disaster Recovery

CTSU has a formal Business Continuity and Disaster Recovery (BCDR) plan that would be used in the event of a significant failure of regular computing services, due to a fire, flood, long-term power outage, or other events that have a major impact on systems operations. The BCDR, Contingency Plan (CP), SSP, and other subsidiary plans, document activation triggers, failover procedures, and communication matrices, among other relevant information, on business continuity and disaster recovery. The plan identifies the primary and backup members of the BCDR team, and other key stakeholders. Disaster Recovery (DR) is initiated by the Assistant Project Director (of Informatics) in consultation with other Assistant Project Directors, and is conducted by the Systems Manager.

2.3.1 Alternate Data Center

In addition to the data centers owned and operated by Westat on premises, CTSU also operates a Virtual Private Cloud (VPC) data center on the Federal Risk and Authorization Management Program (FedRAMP) authorized Amazon Cloud Service Provider (CSP), using Amazon Web Services (AWS). Westat implements the same security policies and best practices on the AWS VPC as it does on the physical data centers. More information on the security apparatus of the underlying cloud infrastructure is available at https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf.

3. Frequently Asked Questions

1) What happens to the patient enrollment forms, which have PII, after it is faxed to CTSU?

The eligibility checklist/enrollment documents are bar-coded for scanning into an image repository. Based on the arrangement with the Lead Protocol Organization (LPO), some of this data is entered and stored in the database. The hard copy forms are placed into folders identified by study, site, patient identification number, and investigator. Folders are filed in a secure location, and archived after two months.

2) Is PII kept anywhere at CTSU, either as a hard copy or in an electronic database?

If a Case Report Form (CRF) requires PII, and if CTSU is responsible for the data entry (for a few studies), then that information would be stored in the OC database. For any CRFs, clinical reports, or other documents received from the sites that contain PII, the hard copy and the electronically scanned copy would be retained by the CTSU. In addition, the CTSU's SDP collects source documents. The documents in the SDP are triaged to make sure that there is no PII. Any document with PII is either redacted or removed from the servers.

3) If PII is kept in an electronic database, has the information system received an Authorization to Operate (ATO) as required by FISMA?

The databases at CTSU are operated in compliance with FISMA and in accordance with NIST Risk Management Framework (RMF) security principles, including identification and authentication, access control, backup and recovery, security patch management, and auditing. Independent third party reviewers regularly conduct a formal Security Control Assessments (SCA) of the CTSU information system, including the database to demonstrate compliance with the FISMA, Office of Management and Budget (OMB) Security of Federal Automated Information Resources, the RMF, and Health and Human Services (HHS) & National Institute of Health (NIH) policies and procedures. Based on this, Westat maintains an active ATO from NCI.

4) Who has access to data containing PII?

Access to PII is limited to those with CTSU project responsibilities that are related to the use of the data. All project staff are required to certify on the Standard Operating Procedures related to data security and confidentiality, and must have signed a confidentiality agreement. For those studies where data management is shared between the CTSU and the LPO, the LPO staff would also have access to the CTSU applications and PII data when appropriate.

5) How is PII protected?

See the Security Policies and Procedures section for details.

6) Are there procedures in place for reporting theft or loss of data containing PII?

Yes. According to Westat Corporate Policy: "Any individual employed or contracted by Westat is encouraged to report any security incident or issue at any time to the appropriate manager, the PC Helpdesk, or the Human Resources Department. Staff are required to report security incidents in which they believe systems security has been, or may be, breached, such as by the unauthorized or suspicious presence of unidentified individuals on Westat premises; unauthorized use of passwords; unauthorized access to a server area or otherwise secure systems area; demonstrated or likely existence of a virus on a computer; and possible unauthorized transmission of confidential data without encryption or security." CTSU project staff at Westat are also required to take the NIH

Information Security and Privacy Awareness Training (ISAT) which further reinforces knowledge of the procedures, as well as potential consequences for not following them.

7) **Is any sensitive data ever taken off site (e.g. on a laptop) for any reason?**

Auditors can access the CRFs through secure web applications. Normally, the data is not taken off site in hardcopy form. If required, paper copies can be made, but they will be shredded after use, by Westat-provided shredders. Normal procedures require that CRF data not be stored on a laptop, if exceptions are requested and granted a Westat laptop with full disk encryption and appropriate security controls is used.

8) **How can I get more information on CTSU WISSP security policy and best practices?**

Please email ctsucontact@westat.com or call 1-888-823-5923 option 1 for the CTSU Helpdesk.

9) **Is OPEN 21 CFR Part 11 compliant?**

Yes. CTSU hired a third party to audit OPEN for compliance with the U.S. Food and Drug Administration's (FDA) Code of Federal Regulations, Title 21, Part 11 (21 CFR Part 11) – Electronic Records; Electronic Signatures. It is the criteria under which electronic records and electronic signatures are considered trustworthy, reliable, and legally equivalent to traditional paper records and handwritten signatures. OPEN was found compliant to applicable requirements of 21 CFR Part 11.

10) **Are CTSU user applications HIPAA compliant?**

Yes, CTSU user applications including OPEN satisfy the HIPAA privacy and security rule requirements. CTSU applications abide by the more comprehensive and strict requirements of the NIST RMF, FISMA compliance, and the NIST Special Publication 800-53 Revision 4 on Security and Privacy Controls for Federal Information Systems and Organizations. CTSU is audited each year by an independent internal security team every year and by a third party assessor every three years. Based on these findings, the CTSU – Enterprise Information Systems owner at NCI issued an Authority to Operate (ATO). By achieving this ATO, CTSU also demonstrates compliance with HIPAA.

11) **What is the FIPS 199 security categorization for CTSU user applications?**

CTSU user applications including OPEN are secured according to laws and guidelines set forth in the FISMA and specifically in NIST Special Publication 800-53 Rev 4, "Recommended Security Controls for Federal Information Systems and Organizations" which requires a Federal Information Processing Standards Publications (FIPS) 199 data sensitivity categorization to ensure the security controls applied are appropriate for the risk. The FIPS categorization for OPEN and CTSU is at the Moderate level, which is appropriate for the sensitivity of the data the system contains. The system has been assessed by an independent third party assessor to ensure the security controls are in place and working as intended. The servers are hosted by Westat and have an authority to operate from NIH per C&A for FISMA-Moderate. Furthermore, Westat maintains a continuous monitoring program of vulnerability identification and remediation. More information about FISMA is available at the NIST website location: https://csrc.nist.gov/Projects/Risk-Management/Detailed-Overview and at the NIST website for Standards for Security Categorization of Federal Information and Information Systems website location: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf.

12) **Are CTSU user applications FIPS 140-2 compliant?**

Yes, CTSU user applications including OPEN are Federal Information Protection Standards (FIPS) 140-2 compliant. This FIPS standard ensures all encryption used for ensuring data confidentiality is implemented at an appropriate level, and effective manner. The application use Transport Layer Security (TLS) (previously the now-deprecated predecessor, Secure Sockets Layer (SSL)) certificates issued by a trusted Certificate Authority (CA), viz. DigiCert Inc. (www.digicert.com) to encrypt data in transit, and server and database encryption is implemented to ensure data is secure at rest. All of the following are FIPS 140-2 compliant.

- Details regarding FIPS 140-2 compliance of SSL certificates issues by DigiCert can be found at http://www.digicert.com/docs/cps/DigiCert_CPS_v301.pdf. Please refer to section 6.2.1 for specifics.
- Details regarding FIPS 140-2 compliance of the Windows server (Microsoft OS) can be found at https://docs.microsoft.com/en-us/windows/security/threat-protection/fips-140-validation.
- Details regarding FIPS 140-2 compliance of the Linux server using RedHat OS can be found at http://www.redhat.com/about/news/press-archive/2013/4/red-hat-completes-fips-1402-certifications.

Revision History			
#	Date	By	Description
01	01/09/2012	Amar Patgiri	Earlier security documents consolidated into a Security Overview document.
02	06/12/2013	Amar Patgiri	Updated and verified for accuracy.
03	03/24/2015	Amar Patgiri Thamizh Thendral Ravi Rajaram	The document was overhauled.
04	4/29/2015	Mark Stauffer	Revised grammar and styles within the document.
05	5/4/2015	Ravi Rajaram	Reformatting
06	5/6/2015	Seshu Cherukuru	QC Review
07	11/23/2016	Ravi Rajaram	21 CFR Part 11 information was added
08	3/23/2017	Thamizh Thendral	Minor updates were made
09	10/13/2017	Thamizh Thendral	FAQ on FISMA classification and FIPS compliance were added.
10	10/4/2018	Thamizh Thendral	Performed Annual review and minor changes were made. The document was QC-ed and suggested updates were made.
11	12/19/2018	Ravi Rajaram	Added info about SDP.
12	7/12/2020	Thamizh Thendral	Performed Annual Review and made minor changes.
13	10/23/2020	Thamizh Thendral	Performed periodic review and added more details. Incorporated feedback and edits from Dennis.
Last Saved By Thamizh Thendral on 10/23/2020 11:30:00 AM			
File Location: \\westat.com\DFS\CTSU6181\TO2\6181.04_Infrastructure\02_Infrastructure\Documentation\SecurityOverview\			