### REDCap API Token Protection for <Project Name>

1. Purpose / Background

This document describes the safeguards in place to secure the REDCap API token(s) used by <project name> to access ePHI stored in the Indiana CTSI REDCap system.

2. Keywords

 ePHI, security, safeguard, paper, electronic

3. Scope

This document spans the <Project Name> environment as well as its interconnection with REDCap.

4. Description

4.1. Project Description:

The <project name> … (describe what the project is about).

4.2. Information System:

The <project name> information architecture and data workflow is as follows (this is just an example – your workflow may be very different):

1. Data is generated (describe where and how) and stored in the Indiana CTSI REDCap system … (briefly describe how).
2. An application <application name> written in <language> consumes REDCap data. (Describe details such as whether it is a web app, what it does, etc.).
3. The application resides on a server called <hostname> in <location> which connects to REDCap to transfer data to the <hostname> server. The server runs <OS name> <version>.
4. A REDCap API token issued by the Indiana CTSI REDCap administrator is used by the application to gain access to REDCap. This token is stored on the server <hostname> in <location>.

5. Application Safeguards

The safeguards described below are divided into physical, administrative, and technical categories as per the HIPAA Security Rule.

* 1. Physical
		1. **Servers**: The <project-name> is hosted on the <hostname> server. See Section 6, Server Safeguards.
	2. Administrative
		1. IU-Wide: IT policies IT-01 through 28, ISPP-24. IU HIPAA Privacy and Security Compliance Plan.
		2. <Department>:
			1. **Incident Response:** See 6.2.3.1
			2. **Problem Escalation:** Problems related to the use of and/or access to <application name> are reported to <who> via email and/or other internal Jira issue ticketing system. In case of an emergency or production system outage, <who> (and/or delegates) are notified and will contact <who> at 317-xxx-xxxx.
			3. **Training:** All personnel connected to the project receive HIPAA training annually, including human subjects research training, as per Indiana University’s HIPAAA Privacy and Security Compliance Plan. It is the responsibility of the project leader and the <eg. Chairman of the Dept. of …> to ensure that the personnel have the required training and the training is up-to-date.
			4. **Business Associate Agreement:** See 6.2.3.4
	3. Technical
		1. Account Management: (If accounts are created for this application, what is the process for creation, review, and deletion? Who decides what accounts are created or deleted and how?).
		2. Authentication: (If accounts are created for this application, how are they authenticated?}
		3. Authorization: (If accounts are created for this application and roles are defined within the application, which roles have access to REDCap and what is the process for assigning or revoking accounts to/from roles? Who decides which accounts have which roles and when?)
		4. Password Management: (What controls are there on passwords? ADS accounts, for instance, follow IU’s strict passphrase-based password strength requirements. If local passwords are stored, how are they protected?).
		5. Access Control: (Is the application restricted by .htaccess entries, CAS, local user accounts, IP-addresses, such as IU-only IP addresses, etc.?)
		6. Remote System Access: (Is the application accessible remotely via http or some other method? Is it an encrypted connection?)
		7. Logging: (Does the application log use/access/activity and/or data inserts/updates/queries/reports/exports? If the application defines users, does it log which user does what? Is use of the API token logged?)
		8. Audit: (Are audits of the application conducted? How, when, by who? Is the application monitored for security and/or privacy breaches? How, when, by who?)
		9. Auto-logouts: (For example: Users are automatically logged out after 30 minutes of inactivity.)
		10. Patching: (What process will you use for identifying and fixing critical issues in the application or the software it depends on?)
		11. Application Scanning: (What application security scanning will you do? For a web application, you must use the UISO Application scanner before going in to production, before any major change, and at least twice a year.)
		12. Data Encryption: (For example) Access to the application is over an encrypted (HTTPS) channel.
		13. Database Management: (For example) All ePHI is stored in the REDCap system hosted by UITS. REDCap is HIPAA aligned.
		14. User Support: See Section 6.3.14, if application support is not different from server support.
		15. Documentation: See Section 6.3.15, if application documentation is not different from server documentation.
		16. Monitoring: The application is monitored using ????. Alerts are issued if the service is down. For escalation, see 6.2.3.2.
		17. Data Export: The REDCap API token will never be stored elsewhere besides REDCap and those servers explicitly covered by this SOP without the express permission of a REDCap administrator. Data will only be provided to those who are allowed to see that data.

6. Server Safeguards

The safeguards described below are divided into physical, administrative, and technical categories as per the HIPAA Security Rule.

* 1. Physical
		1. **Servers**: The <hostname> server uses Indiana University’s Intelligent Infrastructure (II). II is hosted by the Storage and Virtualization (SAV) group within University Information Technology Services (UITS), IU’s central IT organization. Consequently, the physical safeguards UITS has in place apply directly to the server. These include a hardened data center with 24x7 access control, monitoring, etc. The UITS document UITS-ECC-PE describes these physical controls.
	2. Administrative
		1. IU-Wide: IT policies IT-01 through 28, ISPP-24. IU HIPAA Privacy and Security Compliance Plan.
		2. UITS/Enterprise Infrastructure: The Intelligent Infrastructure System Security Plan UITS-SSP-II describes in detail the administrative safeguards SAV has in place to protect ePHI.
		3. <Department>:
			1. **Incident Response:** All IT security incidents/data breaches are reported by <who> to <authority in the dept>, the University Information Security Office, and the Chief HIPAA Privacy and Security Officers as per HIPAA and HITECH regulations.
			2. **Problem Escalation:** Server issues are reported to the system administrator in the <Department>. Intelligent Infrastructure issues are reported to the SAV group via email (sav-request@iu.edu). In case of an emergency or production system outage, <who> (and/or delegates) are notified and will contact <who> at 317-xxx-xxxx.
			3. **Training:** All personnel connected the project receive HIPAA training annually, including human subjects research training, as per Indiana University’s HIPAA Privacy and Security Compliance Plan. It is the responsibility of project leader and the Chairman of the <department> to ensure that the personnel have the required training and the training is up-to-date.
			4. **Business Associate Agreement:** <Applicable only if the server has anything that is vendor supported> There is a HIPAA compliant business associate agreement is currently in place with <vendor> to perform maintenance and support per contractual arrangements**.**

* 1. Technical
		1. Account Management: (Describe how accounts are managed on <server>).
		2. Authentication: (For example) System accounts on the server are delegated to IU’s central ADS authentication system. Server access requires the use of the IU VPN and membership in an ADS security group.
		3. Authorization: (For example) The ADS security groups are managed by <who>, who has responsibility to approve and enable/disable user accounts within these ADS security groups.
		4. Password Management: (For example) ADS accounts follow IU’s strict passphrase strength requirements.
		5. Access Control: (For example) Server access is restricted via (a) individual user accounts, (b) IU’s Data Center firewall, and (c) Linux iptables firewall. The Data Center firewall allows traffic from outside only to ports 80, 8080, 443, and 8443. Access to port 22 (SSH) is restricted to IU-only IP addresses. The Linux iptables firewall further restricts access to the application on port 8443 to specific, user desktop IP addresses, and to port 22 to a single, secure IP address behind the IU Data Center firewall.
		6. Remote System Access: (For example) The system is accessed remotely in two ways: (a) via SSH, and (b) via HTTPS. SSH access is limited to a handful of <Department> IT staff and to authorized end users.
		7. Logging: (For example) All user access to the server is logged. This includes successful and unsuccessful logins.
		8. Application & Server Auditing: (For example) The server audits all successful and unsuccessful logins, all network access (IP numbers), and system processes such as startups/shutdowns, patching, upgrades, etc.
		9. Auto-logouts: (For example) Users are automatically logged out after 30 minutes of inactivity.
		10. Patching: (For example) If a critical vulnerability is detected within the OS, IT staff will take ownership to determine risks, identify a course of action, document, and then facilitate and participate in the process for resolution within an agreed to timeframe.
		11. Server Scanning: The server was scanned using UISO’s host scanner prior to deployment and is routinely scanned after upgrades, patches, or any other change that impacts security.
		12. Data Encryption: (For example) Access to the server is encrypted using SSH. Administrative access to the windows server via RDP is encrypted.
		13. Database Management: (For example) Data are stored locally in a MySQL database which is kept patched on a regular basis.
		14. User Support: Users of the server are supported by the <Department> IT staff via phone, email, or personal visits. The Enterprise Infrastructure Storage and Virtualization group provides support for the underlying VMware environment.
		15. Documentation: The <department> IT unit is documenting its information security practices vis a vis this server. <Department> also maintains extensive documentation regarding its practices generally.
		16. Monitoring: The server is monitored using <software/process>. Alerts are issued if the service is down. Problems are escalated in the manner described in 6.2.3.2.
		17. Data Export: Data will only be provided to those who are allowed to see that data.

*Note: UITS controls for the REDCap service are documented in the REDCap SSP UITS-SSP-REDCap*.

7. Roles & Responsibilities

**Key Personnel** – The <who> is responsible for monitoring and approval of personnel to have access and appropriate permissions to the server and application. The IUSM Associate Dean of Clinical Research is responsible for overseeing the Dept. (if applicable) The security of the underlying cyberinfrastructure is the responsibility of Enterprise Infrastructure’s Director of Systems Infrastructure. The <department> IT group provides system administration for server. The <application name>application is administered by <who>.

The <who> approves this SOP and any future modifications will be reviewed and approved by him/her and <who else>. All modifications are documented in this document.

**Contact Information**

<department>:

 <name>

 Chairman, <department>

 <email>

 <phone>

 Richard Kovacs, MD

 IUSM Associate Dean of Clinical Research

 Associate Director, Indiana CTSI

 rkovacs@iupui.edu

 (317)-962-0142

 <name>

 Project Owner

 <email>

 <phone>

<name>

 System Administrator

 <email>

 <phone>

UITS:

Richard Meraz

 Manager, Advanced Biomedical IT Core

 rfmeraz@iu.edu

 (317) 274-3338

8. Training

Individuals mentioned in this SOP that handle ePHI have been properly HIPAA trained and have had human subjects research training, addressing IU’s HIPAA Privacy and Security Compliance Plan, Section 5 – Safeguards, 2.2 Administrative, 2.2.3.5 Training.

9. Monitoring Requirements

This SOP must be reviewed twice a year. Changes should be made appropriately and approved.

10. Record Management

An electronic version of this SOP is maintained securely by UITS and <department> and reviewed semi-annually.

11. References

**11.1. Policies & Plans**

 IU IT Policies IT-01 through IT-21, ISPP-24

 <http://protect.iu.edu/cybersecurity/policies>

 IU HIPAA Privacy and Security Compliance Plan

<http://researchadmin.iu.edu/HIPAA/hipaa_docs/IU_HIPAA_Compliance_Plan_Final_Combined.pdf>

**11.2. Standards**

 NIST 800-53:

 [http://csrc.nist.gov/publications/nistpubs/800-53- Rev2/sp800-53-rev2-final.pdf](http://csrc.nist.gov/publications/nistpubs/800-53-%20%20%20Rev2/sp800-53-rev2-final.pdf)

**11.3. URLs**

 None.

**11.4 Other Documents Referred to in this SOP**

11.4.1. UITS-ECC-PE

11.4.2. UITS-SSP-II

11.4.3 UITS-SSP-REDCap

 <add as appropriate>

**11.5. Compliance**

This SOP addresses HIPAA Rule §164.308(b)(1): Administrative Safeguards – Business Associate Contracts & Other Arrangements – Written Contracts or Other Arrangements (R). It also addresses Indiana University’s HIPAA Privacy and Security Compliance Plan.

**11.6. Supplementary Documents**

<add as appropriate>

12. Definitions

ePHI Electronic protected health information: All individually identifiable health information related to a patient that is created, maintained, or transmitted electronically.

13. Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| #  | VERSION  | DESCRIPTION  | DATE  |
| 1  | V 1.0  | Initial  | <date>  |

14. Appendix A

Users with Privileged Access to the Application/Servers

|  |  |  |
| --- | --- | --- |
| Name | User Category | Group |
| Name | Application Administrator | <Department> |
| Name | System Administrator | <Department> |
| Name | Vendor End-User Support | Vendor Name |
| UITS EI-SAV Team per Troy Williams | System Administrator | Enterprise Infrastructure, UITS |
| UITS RT-ABITC Team per Richard Meraz | REDCap Administrator | Research Technologies, UITS |