|  |  |
| --- | --- |
|  | **Date Submitted:**      (please enter date format yyyy-mm-dd) |

**Information Security Risk Assessment:
Third Party**

**Request Number:**

**Risk Assessment ID:**

**Additional Assessment Recipients:**

**Instructions:** Please complete the Risk Assessment Questionnaire and Attachments and return it to the Office of Information Security. Incomplete submissions may result in delays. Do not reference features and settings that will not be present and enabled at implementation. If you have any questions or need clarification, please contact us. This is not a pass or fail document, rather it is a discovery document that benefits the party being assessed and the WashU Community by identifying risks enabling mitigation and helps to protect data. Many questions can be answered by reviewing[**Appendix A**](#Appendix)**.**

|  |
| --- |
| **General Information- Owner(s)/ Sponsor** |

**WashU Contact**

**Name:**

**Title:**

**Contact Number:**

**Email:**

**Date Completed:** **2017-05-17**

**Data Owner**

**Name:**

**Contact Number:**

**Email:**

**Data Custodian**

**Name:**

**Contact Number:**

**Email:**

**Technical Lead**

**Name:****Contact Number:**

**Email:**

**Sponsor/Vendor**

**Name(s):**

**Email(s):**

**Contact Number(s):**

|  |
| --- |
| **Service Information** |

**Provide a brief description of the function or service your organization is providing to WashU:**

**Identify the WashU schools or departments that will utilize this function or service:**

**Will any physical or logical modification(s) to existing WashU hardware/software infrastructure be required?**

[ ]  Yes [ ]  No

**If so, please describe the modification(s) and explain why they are required.**

**If this is a vendor hosted solution, does the vendor use any third-party hosting services?** [ ]  Yes [ ]  No

* **If yes, please list below.**

|  |
| --- |
| **Application Information** |

**If one or more computer applications are used to facilitate the service; provide computer application names, versions, and descriptions:**

**Were computer applications developed internally or by an external third-party?** [ ] Internal [ ] External

* **Please explain below:**

**Is any Freeware, Shareware, or Open Source software used to facilitate the provided service?** [ ] Yes [ ] No

* **If yes, please list below.**

**What types of data will the application receive, store, process and transmit?**

* **[ ]  Protected Health Information (ePHI)**
* **[ ]  Credit Card (PCI)**
* **[ ]  Other (specify in comments)**

**Please explain the process below:**

**How many transactions will be processed on a daily basis (approx.)?**

* **[ ]  1-100**
* **[ ]  101-500**
* **[ ]  501-1000**
* **[ ]  More than 1000**

**Please explain transactions below:**

**Does the application require user authentication?** [ ] Yes [ ] No

**If “Yes” are user credentials stored locally, or in a reusable credential store? (e.g. LDAP, Active Directory).**[ ] Yes [ ] No

**Will logging be enabled for specific activity and events?** [ ] Yes [ ] No

* **If “Yes”, please list and describe the audit functions below (e.g., user access, patient view); if “No”, explain why:**

**If application contains ePHI, do you perform a HIPAA Risk Assessment as prescribed by OCR regulations?**

[ ] Yes [ ] No

* **If “Yes” please state below:**

|  |
| --- |
| **Data Protection Information** |

**Where will WashU data be located?**

* **Host Name:**
* **City:**
* **State:**
* **Country:**

**Can the asset be replaced?** [ ] Yes [ ] No

**Will any WashU Data be transferred to locations or viewed by persons outside of the United States?**
[ ] Yes [ ] No

* **If “Yes” describe below:**

**What is the data retention policy for this data? Please explain below:**

**Do you have a documented policy that communicated how you will monitor your system(s) and notify WashU of security events?** [ ] Yes [ ] No

* **If “Yes” describe below:**

**Will data at rest be encrypted?** [ ] Yes [ ] No

* **If “Yes” specify the encryption algorithm/method and key length used below:**

**Answer “Yes” or “No” and provide explanation as necessary for each of the following statements regarding encryption key management policy and procedures:**

* **Only strong keys are created and controls are in place to prevent unauthorized key substitution. [ ]  Yes [ ]  No**
	+ **If “Yes” please describe:**
* **Keys are distributed only to authorized custodians or authorized key management devices. [ ]  Yes [ ]  No**
	+ **If “Yes” please describe:**
* **Keys are never distributed in the clear. [ ]  Yes [ ]  No**
	+ **If “Yes” please describe:**
* **Stored keys are encrypted and key-encrypting keys are stored separate from data-encrypting keys.[ ]  Yes [ ]  No**
	+ **If “Yes” please describe:**
* **Keys are changed at the end of the defined crypto period. [ ]  Yes [ ]  No**
	+ **If “Yes” specify the time period:**
* **Any key whose integrity has been, or is subject of having been, weakened or compromised is securely retired and a new key is created. [ ]  Yes [ ]  No**
	+ **If “Yes” please describe:**
* **Are keys changed whenever a key custodian or person with access to encryption keys leave the organization.
[ ]  Yes [ ]  No**
	+ **If “Yes” please describe:**

**Will data in transit (e.g., server-to-server, client-to-server, etc.) be encrypted? [ ]  Yes [ ]  No**

* + **If “Yes” specify the protocol, version, encryption algorithm/ method, and key length used below:**

**If SSL certificates will be used to encrypt communications they will use SHA-2 hashing instead of SHA-1, which is no longer considered secure and being depreciated by web browsers? [ ]  Yes [ ]  No**

* + **If “No” please explain why:**

**Will the application be supporting internal or external data transmissions? [ ]  Yes [ ]  No**

* + **If “Yes” please answer the following:**
		- **What is the purpose of the transmission?**
		- **What is the transmission method?**
		- **What/Who is the transmission recipient?**

**Will application utilize tracking cookies? [ ]  Yes [ ]  No**

* + **If “Yes” please answer the following:**
		- **Explain the type and purpose for each cookie:**
		- **What data and metadata (e.g. referring URL) will be collected?:**
			* **How will the data be used?:**
			* **Is the data or and subset of it shared with a third-party(s) [ ]  Yes [ ]  No**
				+ **If “Yes” please answer the following:**

**With whom?**

**What data?**

**Do the servers have antivirus protection? [ ]  Yes [ ]  No**

* + **If “Yes” please answer the following:**
		- **Who is the vendor?**
		- **What is the product?**

**Is a mobile device management system used to track and manage mobile devices (laptops, tablets, and smartphones)?** [ ] Yes [ ] No

* + **If “Yes” what is the system?:**

|  |
| --- |
| **Backup/ Disaster Recovery** |

**Will back-up operations be able to run concurrently with operation of the application? [ ]  Yes [ ]  No**

* + **If “No” please explain:**

**Do your organizations have a Disaster Recovery Plan that describes how the application and data will be recovered in the event of an emergency? [ ]  Yes [ ]  No**

**Have you shared the Disaster Recovery plan with WashU? [ ]  Yes [ ]  No**

* + **If “No” please provide where it is located:**

**Is a process in place to notify WashU of alerts or potential security breach issues? [ ]  Yes [ ]  No**

* + **Please explain the process:**

|  |
| --- |
| **Business Partner Information** |

**Is your organization privately owned or publicly held?** [ ] Private [ ] Public

**How many individuals does your organization employ?:**

**Does your organization have an information Security Department?** [ ] Yes [ ] No

* + **If “Yes” please provide contact information:**

**Are your personal trained information security practices and requirements, such as payment card industry (PCI) standards, or HIPAA training if ePHI will be handled?** [ ] Yes [ ] No

**How often do personnel receive security training?:**

**Does your organization hold any of the following certifications? If yes please provide verification information for each along with the Risk assessment as a supplement.**

* [ ] Yes [ ] No **PCI-DSS Certification**
* [ ] Yes [ ] No **HITRUST CSF Validated? CSF Certified**
* [ ] Yes [ ] No **ISO 27001**
* [ ] Yes [ ] No **Other (specify in comments)**
	+ **If “Other” explain list below:**

**Do you have a Statement on Auditing Standards (SAS), Statement on Standards for Attestation Engagements (SSAE) or equivalent?** [ ] Yes [ ] No

* + **If “Yes” please provide that documentation with the completed risk assessment as a supplement.**

**Are vendors and/ or employees permitted to remotely access resources within your network?** [ ] Yes [ ] No

* + **If “Yes” please describe the controls below:**

|  |
| --- |
| **Attachment A(Architecture Diagram)** |

**Instructions:** Provide a graphic representation of the application architecture and data flow. Be as specific as possible and include physical locations, logical locations, IP Addresses, Operating Systems/ versions, system interconnections, key incoming and outgoing data flows, security controls in place (ex. Encryption). You may attach a single hybrid diagram or multiple specific diagrams to summarize the architecture and key data flows.

|  |
| --- |
| **Appendix A** |

**Office of Information Security Contact Information:**

* Email: infosec@wustl.edu | Contact Number: 314-747-2955

**All Protected Health Information:**

* Must be encrypted

**Definitions:**

* Questionnaire Owner- has the responsibility to complete the form for the asset to be assessed.
* Data Owner- has administrative control and has been officially designated as accountable for a specific information asset dataset.
* Business Owner/ Sponsor- has the overall ownership of the asset.
* PHI- patient name, date of birth, date of service, MRN, invoice number, social security number, address, email address, facial photos or other identifying photos or numbers.

**Helpful Links:**

* <https://informationsecurity.wustl.edu>
* <https://informationsecurity.wustl.edu/resources/glossary-of-terms/>
* <https://informationsecurity.wustl.edu/resources/information-security-solutions/data-classification/>

**\*Below Completed by the Office of Information Security**

|  |
| --- |
| **Assessment of Risk** |
| **Date:**       | **Assessment ID:**      |
| **Asset(s) Assessed:**       |
| **Risk Rating:** [ ]  **Low** [ ]  Medium [ ]  High  |
| **Requested by:**       |
| **Status:**       |

|  |
| --- |
| **Assessor’s Information** |
| **Name:**       | **Title:**       |
| **Contact Number:**       | **Email:**       |

|  |
| --- |
| **Review Notes** |

\*If this page is not sufficient please complete on the [Continued Review Notes](#ConReviewNotes) page.

**Background:**

**Identify and Describe Risks:**

|  |
| --- |
| **Acceptance of Risk** |

**Explanation:** The Office of Information Securitywill report all risks and provide explanations to the party being accessed. The number one mission of Information Security is to strive to provide the highest level of risk mitigation while not impeding the business unit. This includes Information Security working with all parties to try to develop a compromise for risk. Some risks may be deemed High, if a party doesn’t see a compromise that can be made they may choose to accept the Risk. A signature from the Information Security Office and a Signature of the Business Owner is **required**. This ensures the risk was communicated and all liability is taken on by the Business Owner.

**Acceptance of Risk:**

Information Security Signature:

Business Owner Signature:

|  |
| --- |
| **Continued Review Notes** |