

**Cybersecurity Department**

**Software Vendor Assessment Form**

[This Governance process applies to Projects, Maintenance tasks, Changes, Releases, Decision Support, Risk, Security, Compliance & Exception Management Control(s)]

**Table of Contents**

[**Software vendor assessment form purpose & description 3**](#_30j0zll)

[**Basic application/system information 4**](#_1fob9te)

[**Data management and integration 5**](#_3znysh7)

[**Authentication/authorization/access manage 6**](#_2et92p0)

[**Account and password management 7**](#_tyjcwt)

[**Network access and data protection 8**](#_3dy6vkm)

[**Auditing/logging/monitoring 9**](#_1t3h5sf)

[**Physical security 10**](#_4d34og8)

[**Vulnerability and threat management 11**](#_2s8eyo1)

[**Availability/backup/recovery 12**](#_17dp8vu)

[**Changement management 13**](#_3rdcrjn)

[**Compliance 14**](#_26in1rg)

[**International operation 15**](#_lnxbz9)

[**Document revision history 16**](#_35nkun2)

# Software Vendor Assessment Form Purpose & Description

BRLI operates in a highly regulated business environment requiring us to conduct business in a rick managed manor. The *Software Vendor Assessment Form* addresses implementation specifications for Information Security Risk Management requirements of CFR 164.308(a)(1)(i). It further assists the BRLI Cybersecurity team in assessing controls implemented by cloud vendors and business affiliates entrusted to process, store, and/or transmit PHI / PII on behalf of BRLI and its members.

Failure to thoroughly answer this questionnaire or incomplete responses will delay the evaluation process and may impact BRLI’s ability to exchange data with your company. Please respond to all questions (indicate "NA" where not applicable). Missing information or incomplete responses will delay the evaluation process.

This assessment process satisfies HIPAA, PCI DSS, and other compliance Security and Risk requirements.

|  |  |  |
| --- | --- | --- |
| **BASIC APPLICATION/SYSTEM INFORMATION** | |  |
| **Question** | **Response** | | |
| 1. Company name: | Prognos Health Inc. | | |
| 1. Primary point of contact (name, phone, email): | Mark Reis VP Business Development, Lab Markets | | |
| 1. Application name: | Opal De-Identification Software | | |
| 1. Description of application: | De-Identification of all PHI and PII | | |
| 1. Who will use the application? | Bioreference IT Staff | | |
| 1. Operating system and version: | Data Dictionary v2.2 Multiple OS supported | | |
| 1. Database type/versions supported: | Flexible | | |
| 1. Database type/version in which application is developed: | It’s not a database based application, it’s developed in Go, a general language. | | |
| 1. Server requirements (if local hosting): | 250 HDD, 16GB RAM, 4 CORE PROCESSOR | | |
| 1. Networking requirement | None | | |
| 1. Web browser requirements: | None | | |
| 1. Other system requirements: | JAVA for ALT engine operation | | |
| 1. What support do you provide for this system/application and its users? | Demo, Initial Configuration, Troubleshooting/Error Debugging | | |
| 1. What are your support hours? | 8am to 6pm M-F | | |
| 1. What is the average response time for support calls? | Within 24 hours | | |
| 1. What support will BRLI be responsible for providing for the system/application and its users? | The application runs on your systems. We provide guidelines of requirements for systems and explanations of process requirements, but we cannot directly support the application within your environment. We’re here to help as much as we can. | | |

|  |  |  |
| --- | --- | --- |
| **DATA MANAGEMENT AND INTEGRATION** | |  |
| **Question** | **Response** | | |
| 1. What type of data will be stored, transmitted, or accessed by this system/application? | PHI or PII will be fed into the application, de-identified data exits the system and is then transferred to us. | | |
| 1. Indicate if the following data types will be stored, transmitted, or accessed by this application/system: |  | | |
| * 1. Protected Health Information (PHI) | Yes (incoming, controlled by BRL) | | |
| * 1. Protected Health Information (PHI) | Yes (incoming, controlled by BRL) | | |
| * 1. Payment Card Industry (PCI) | No | | |
| * 1. Other financial information | No | | |
| * 1. Family Educational Rights and Privacy Act (FERPA) | No | | |
| * 1. Intellectual property | No | | |
| * 1. Research data | No | | |
| 1. Where will this data be stored? | Incoming data remains on your premises. Output is sent to us by you. The output is stored in Prognos’ compliant systems. | | |
| 1. Who will have access to this data (i.e., vendor, faculty, staff, students, public, etc.)? | Only BRLI has access to the data through Opal. The software sits behind BRLl’s firewall and is transmitted to Prognos by BRLI | | |
| 1. How will this data be accessed (e.g., application interface, web portal, or third party application)? | Data is extracted from BRLI internal data sources and sent to the Opal input folder for De-ID processing. | | |
| 1. Does this application or system use cloud services? | No | | |
| 1. Are users of the system able to download/extract data to their local machines? | The system is a production system that does not support an implied “user” model. Since it runs entirely within BRLI systems, BRLI controls all access to the software/system. | | |
| 1. Describe any integration requirements that require exchanging data with other BRLI systems. | Integration is via moving data files to a specific location for Opal to process. The output files are similarly configured. | | |
| 1. Will a user-data import/integration be required to populate the system? If so: |  | | |
| * 1. What file formats are acceptable (e.g., CSV)? Attach interface documentation if available. | Pipe delimited files with the .csv extension | | |
| * 1. Can the import be automated, and if so, for what intervals (e.g., real time, daily, weekly, etc.)? | Yes, we ask that only the output results file import process be automated on a weekly basis (Sundays) | | |
| * 1. What are the acceptable import-file delivery methods (e.g., SFTP, APIs, Ellucian Ethos)? | Prognos SFTP | | |
| * 1. Will the planned data exchange be uni-directional only (from BRLI systems to your application/system), or is a bi-directional integration available, desired or needed? | Uni-directional  From BRLI to Prognos Intake SFTP | | |
| * 1. What type of data will be required to populate the system (e.g., student data, employee data)? | Lab Testing | | |

|  |  |  |
| --- | --- | --- |
| **AUTHENTICATION/AUTHORIZATION/ACCESS MANAGE** | |  |
| **Question** | **Response** | | |
| 1. What are the integration requirements for authentication/ authorization (e.g., LDAP, SAML, CAS, Shibboleth, Active, Directory (AD), etc.)? | N/A Opal does integrate in this fashion. It is a command line application. | | |
| 1. What methods of authentication can be used to authenticate users to the system application? | Only BRLI staff will have access to the system, authentication methods will be implemented by BRL | | |
| 1. Is there additional cost for authentication setup? | N/A | | |
| 1. What user access control mechanisms does the system/application provide (e.g., role-based access)? Include internal application access controls as well. | Opsl is a command line application. | | |
| 1. Provide a list of all accounts required to manage the system and/or application, along with who is responsible for each account. | N/A | | |
| 1. Who (e.g. vendor, BRLI) is responsible for provisioning user access (i.e., adding/modifying/removing) to the system and application? | BRLI | | |
| 1. How does your organization manage accountability for generic accounts and functional IDs? | N/A (no generic accounts are used and if at all we may need, an exception has to be raised and discussed in the infosec committee for approval | | |
| 1. List the security controls that are in place to prevent unauthorized access by other customers or third parties to BRLI data housed in this system/application. | Software is installed at BRLI, neither Prognos nor it’s Trusted Third Party will have access to the software. Only BRLI appointed staff will have access | | |

|  |  |  |
| --- | --- | --- |
| **ACCOUNT AND PASSWORD MANAGEMENT** | |  |
| **Question** | **Response** | | |
| 1. FOR INTERNAL PASSWORD MANAGEMENT ONLY: Describe the system/application’s password requirements (e.g., re-use, required character types, etc.) | N/A Opal itself does not have a password mechanism. Access to the system on which it is installed is controlled by BRL password policies and controls. | | |
| 1. Does the system/application require initial password change after a user’s first login? | N/A Opal itself does not have a password mechanism. Access to the system on which it is installed is controlled by BRL password policies and controls. | | |
| 1. Is the system/application configured with the following account security standards: | N/A Opal itself does not have a password mechanism. Access to the system on which it is installed is controlled by BRL password policies and controls. | | |
| * 1. Account lockout after no more than 6 failed logon attempts |  | | |
| * 1. Lockout duration of at least 30 minutes or until an administrator resets the account |  | | |
| * 1. User session inactivity expiration timeout duration |  | | |
| 1. Are passwords encrypted during transit? | N/A There are no Opal passwords to encrypt. All other external communication is encrypted. | | |

|  |  |  |
| --- | --- | --- |
| **NETWORK ACCESS AND DATA PROTECTION** | |  |
| **Question** | **Response** | | |
| 1. Provide system architecture documentation, including a network diagram of the system and external connections. IP and sensitive vendor information may be omitted. | Refer <https://drive.google.com/drive/folders/1JTgGAsEZ7-FI1h679kWirkmLnVZWyExU>  1)Opal User Manual  2) Network Diagram | | |
| 1. List the certificate authority (trusted third party) that signs your digital certificate. | **Neomind Labs** is the trusted third party used to hold a “key seed” for us and deliver that securely to designated data vendors | | |
| 1. List the network protocols or ports required for this system/application. | SFTP Port:7000 | | |
| 1. List the protocols used by the system to encrypt data in transit. | Hashing tokens are encrypted during SFTP transmission | | |
| 1. For data encryption at rest, provide the following:    1. Encryption vendor    2. Encryption algorithm that is implemented    3. Is the encryption module FIPS 140-2 validated? | 1. AWS 2. AES 128 bit with 256 bit Key 3. AES (Advanced Encryption Standard) adopted by the US government is FIPS 140-2 Validated | | |
| 1. For the enforcement of encryption on portable devices containing sensitive data, provide the following: 2. Encryption vendor 3. Encryption algorithm that is implemented 4. Is the encryption module FIPS 140-2 validated? | No portable device can store or transmit sensitive data like PHI or PII however the end points are also encrypted   1. FileVault disk encryption for MAC and Bit locker for Windows 2. AES 128 bit with 256 bit encryption key 3. Both FileVault and Bitlocker is FIPS 140-2 Validated and compliant | | |
| 1. Are backups encrypted? | N/A | | |
| 1. What is the backup frequency and schedule? | N/A | | |
| 1. Will access to this application be limited to networks identified by BRLI? | Yes, The Opal software is installed at BRLI with no access granted to outside sources | | |
| 1. How are logs secured from tampering? | BRLI will set permission levels internally | | |
| 1. If not connecting directly to the network, will the application communicate with or connect to other devices currently on the network? | No | | |
| 1. For remote customer support, describe how you plan to connect to BRLI's computing environment. | At no time will Prognos require access to BRLI server for debugging and error support. | | |
| 1. Is the application's database in a shared/clustered environment? | No | | |
| 1. If your company allows access to servers and data from the company’s wireless network, how is that access secured? | N/A | | |
| 1. What systems can connect directly to the database(s)? | N/A | | |
| 1. How is administrative access to servers restricted (by user, by role, by device or some combination of these)? | BRLI to set administrative access to the server where Opal will be installed | | |
| 1. Are systems in place to prevent data ex-filtration via the network or a physical device (e.g., USB drive)? | BRLI to set security parameters | | |
| 1. Are there any instances when the application/system is required to use an unsecure service (e.g., ftp) or otherwise store or transmit passwords in clear text? | No, The software does not SFTP any files nor requires any unsecure service. BRLI has full control of any files copied to the server and any files SFTP | | |
| **AUDITING/LOGGING/MONITORING** | |  |
| **Question** | **Response** | | |
| 1. Is the system/application configured to log privileged account access (e.g., super-user, administrator, and root) including accesses, updates, creates and deletes? | No, BRLI controls the application and will monitor who accesses the system | | |
| 1. Does the system/application maintain a secure audit record each time a user accesses, updates, creates, or deletes information? If so, does the audit records contain the following information: | BRLI to monitor and maintain a secure audit record each time a user accesses, updates, creates, or deletes information | | |
| * 1. Unique user identifier | N/A | | |
| * 1. A unique data subject (e.g. patient) identifier | N/A | | |
| * 1. The function performed by the user | N/A | | |
| * 1. The time and date that the function was performed | N/A | | |
| 1. How long are logs retained? Are they available to BRLI upon request? | At BRLI discretion | | |
| 1. How is the system monitored for suspicious activity? How often are logs reviewed? | As only BRLI will be able to access the software, monitoring for suspicious activity to be implemented by BRLI | | |

|  |  |  |
| --- | --- | --- |
| **PHYSICAL SECURITY** | |  |
| **Question** | **Response** | | |
| 1. Describe the physical security controls in place where the system infrastructure is located. | Software install at BRLI, no other outside sources will have access including Prognos | | |
| 1. Does your organization maintain a log of users who enter the data center and their reason for entry? | Software install at BRLI, no other outside sources will have access including Prognos | | |
| 1. How do you enforce secure destruction of electronic media or hard copy of sensitive or regulated data? | Software install at BRLI, no other outside sources will have access including Prognos | | |

|  |  |  |
| --- | --- | --- |
| **VULNERABILITY AND THREAT MANAGEMENT** | |  |
| **Question** | **Response** | | |
| 1. Who will be responsible for maintaining the system updates with the latest security patches or hotfixes? | Prognos will work in conjunction with BRLI for maintaining the system updates with the latest hotfixes. Security patches for the server will be the responsibility of BRLI | | |
| 1. List the product(s) deployed to protect your systems and application against viruses and malware. | Software installed at BRLI | | |
| 1. Does your organization perform regular security vulnerability scanning? If so, provide a summary report of your last scan. | Software installed at BRLI | | |
| 1. Has your organization performed a security penetration test on your environment? If so, provide an executive summary report of your last test. | Refer 2018\_Nov\_Prognos\_Internal\_pentest.pdf <https://drive.google.com/drive/u/1/folders/1JTgGAsEZ7-FI1h679kWirkmLnVZWyExU> | | |
| 1. Do you use any tools to specifically test the security of web applications you develop? | Software installed at BRLI | | |

|  |  |  |
| --- | --- | --- |
| **AVAILABILITY/BACKUP/RECOVERY** | |  |
| **Question** | **Response** | | |
| 1. What mechanisms are in place to address fault tolerance and high availability of this system? Provide your Continuity of Business document. | Software install at BRLI | | |
| 1. Who will be responsible for the backup and recovery process? | Software install at BRLI, BRLI will implement a disaster recovery and backup process | | |
| 1. What is the expected recovery time in the event of an unexpected outage? | Software install at BRLI, BRLI will implement a disaster recovery and backup process | | |
| 1. Is disaster recovery provided? If so, what are the recovery point objective and recovery time objective? | Software install at BRLI, BRLI will implement a disaster recovery and backup process | | |
| 1. Is there additional cost for disaster recovery? If so, what is that cost? | Software install at BRLI, BRLI will implement a disaster recovery and backup process | | |
| 1. Will the recovery or replacement device have the same IT /Security needs as the original system? | Yes, Prognos can provide the software if necessary. | | |

|  |  |  |
| --- | --- | --- |
| **CHANGEMENT MANAGEMENT** | |  |
| **Question** | **Response** | | |
| 1. Describe your standard change management process. | Changes to the system/application goes through a proper change management process which is discussed in the Information security committee meeting for the risk and impact. A ticket is logged by the requester with the business justification and SoD (Segregation of Duties) is followed till the closure. Requester, implementer and approver can not be the same | | |
| 1. How are staff changes handled? Specifically, what is the process for removing staff access when they leave? | Access is removed within 24 hours of staff termination | | |
| 1. Do you have a segregated environment for Development, User Acceptance Testing (UAT), and Production? | Yes | | |
| 1. How do you notify clients and staff when a system/application change is to be implemented? | Clients and staff are notified through E-mails or Slack channel | | |

|  |  |  |
| --- | --- | --- |
| **COMPLIANCE** | |  |
| **Question** | **Response** | | |
| 1. Does your organization require employees to take annual security and privacy awareness training? | Yes | | |
| 1. Does your organization require a background check for employees? | Yes | | |
| 1. What processes does your organization have in place to comply with applicable laws, regulations, and industry standards? Attach any applicable certifications (e.g., HITRUST, PCI DSS, SAS70/SSAE 16 Type, II etc.). | We have a HITRUST certification for our PHI products. It does not cover our de-identification software or use of de-identified data. To ensure HIPAA compliance with our de-identified data and software, we have obtained expert’s determinations in accordance with 45 CFR 164.514(b)(1) | | |
| 1. Do you have an incident response plan and a breach notification process? | Yes | | |
| 1. Can you provide documentation that details the operation, architecture and administration of the system/application? | The Opal User Guide has been provided to BRLI | | |
| 1. Is the application/system compliant with the Americans with Disabilities Act, standard WCAG 2.0 AA? | N/A Opal is not designed for interaction. It relies on the system it’s installed on for compliance in this manner. | | |

|  |  |  |
| --- | --- | --- |
| **INTERNATIONAL OPERATION** | |  |
| **Question** | **Response** | | |
| 1. Does your organization have any international operations? | No | | |
| 1. Does your organization partner with any vendors or contractors with international operations? | Yes | | |
| 1. In what countries do your international employees, vendors, or contractors have operations? | All employees operate in the United States. We have full time contractors based in Bangalore, India | | |
| 1. Describe your systems, applications, and data that your international employees, vendors, or contractors are able to access AND their access method(s). | International contractors are technically and administratively prohibited from accessing PHI. All data (both PHI and de-identified data) is stored in the United States. Certain de-identified and non-confidential data stored in the United States is accessible by international contractors. | | |
| 1. What IT security controls are implemented to ensure that data is transmitted securely with your international employees, vendors, or contractors? | No data is transmitted internationally | | |
| 1. What IT security controls are implemented to ensure that data is securely stored on the systems of your international employees, vendors, or contractors? | No data is stored internationally | | |
| 1. Provide the vendor names, product names, and versions of the workstation antivirus and encryption software used by your international employees, vendors, or contractors. | Impelsys Inc -  **OS** - Windows 10, **Antivirus** - Windows Defender which is updated every 24 Hrs for the latest definitions **Disk Level Encryption** - Bit Locker | | |

**Document Revision History**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Filename** | **Version** | **Date** | **Description** | **Author** | **Phone** | **Email** |
| **Software Vendor Assessment Form** | 1.0 | 11/1/2018 | Initial creation | Charlie Frank | Ext. 7546 | Charli.Frank@bioreference.com |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |