Indiana University Health, Inc. Standard Information Security Requirements and Demonstration of Compliance

These are minimum requirements required by IU Health’s Information Security Program. We recognize that sound practices require continual assessment of evolving risks, technology and relevant issues related to information security. For the purposes of below, (i) each reference to “Agreement” shall be defined to include the BAA and Service Agreement, (ii) each reference to “Provider” shall be defined to include Business Associate, and (iii) each reference to “IU Health” shall be defined to include Covered Entity.

Any information technology system implemented as part of this Agreement that processes, stores, transmits, or receives information classified as Restricted or Critical by the IU Health Data Classification Policy is subject to the regulatory provisions regarding these data classifications, which include the Health Information Portability and Accountability Act (HIPAA), Family Educational Rights and Privacy Act (FERPA), and the HITECH Act. Therefore, any such system implemented as part of this Agreement must:

i. Demonstrate that it stores data at rest in compliance with the HIPAA Security Rule or industry best practices as applicable by either utilizing existing Provider’s facilities (e.g., storage area network, file servers) to store data, or utilizes NIST FIPS 140-2 compliant encryption to store it local to the system itself.

ii. Demonstrate that it is able to securely transmit and receive PHI in compliance with the HIPAA Security Rule, or HITECH Act, by utilizing NIST FIPS 140-2 compliant encryption.

iii. Demonstrate that data access requires a unique username/password or two-factor authentication (e.g., username and password, along with a personal identification number, certificate, software or hardware token, or smart card).
   1. Ideally, the system will demonstrate that users can be provisioned or federated from already-existing directory systems utilizing either LDAP/S or Identity Management technologies such as Active Directory, OpenAthens, Shibboleth, or login.gov through Active Directory Federation Services or other integration technologies including Security Assertion Markup Language (SAML) version 2.0 or greater.
   2. If a third-party system is utilized in the federation process, Vendor will have reasonably and appropriately assessed and addressed risks with said system and assumes liability for any breach of login credentials caused by the third-party federation provider providing services on behalf of Vendor in service to IU Health. Vendor will also provide evidence of compliance and security, including Service Organizational Controls Level II (SOC2) reports, Health Information Trust (HITRUST) Common Security Framework (CSF) certification, ISO 27001/27017/27018 certification, or a third-party Risk Assessment completed by a certified Information Security professional or licensed Certified Public Accountant.

iv. Provide the ability to log and monitor access to data
   1. Log the date, time, user id, requesting Internet Protocol (IP) address, subject ID(s), and actions taken by users to query, read, add, modify, or delete data about said subject(s).
   2. Provide the ability to query the logging and monitoring data by user, date, workstation or subject, or export said data in a structured format for reporting purposes.
3. Provide the ability to export the data so that IU Health can retain it in accordance with the Center for Medicare and Medicaid Services’ Office of Civil Rights (OCR) guidance on Cloud Computing, and internal IU Health policies on data retention.
   a. Ideally, the system would allow IU Health to receive the data over syslog or a similar protocol allowing it to be transmitted to the hosted Security Incident and Event Manager (SIEM).

v. Allow installation of IU Health supplied digital certificates and certificate chains to facilitate encryption utilizing Transport Layer Security (TLS) version 1.2 or greater technologies.
   1. If the system does not support TLS 1.2 or greater, please document the resolution and steps to update the system to handle it with an estimated completion date.

vi. Demonstrate overall systems compliance by providing the following for mandatory review by IU Health’s Information Security Team:
   1. An overall system architecture diagram, which includes a demonstration of logical separation of client data that prevents commingling of data.
   2. A recommended network architecture implementation, including recommended segmentation, firewall rules, and network protection such as Data Loss Prevention to allow only applicable ports & protocols to protect data.
   3. A documented example of an actual system implementation.
   4. If this is a cloud-based or hosted system, a documented network architecture showing the security controls in place (e.g., firewalls, IDS/IPS, authentication, Data Loss Prevention, etc.).
   5. Demonstrated reviews of firewall and Web Application Firewall (WAF) configurations to validate and verify minimum necessary rules are in place and that misconfigurations which can allow unauthorized access are avoided.
   6. Demonstrated security scanning of the environment that includes credentialed and non-credentialed vulnerability scans of the internal and external environments, with a specific focus on addressing Server-Side Request Forgery (SSRF) and Cross-Site Request Forgery (CSRF) issues.
   7. Storage of Restricted or Critical data behind a stateful network firewall, ideally logically segmented and not stored on a device with a directly Internet-accessible Internet Protocol (IP) or Internet Protocol v6 (IPv6) address.
   8. Demonstrated backup and recovery procedures.
   9. Demonstrated user access management procedures.
   10. Static code analysis utilizing a verified third-party tool to ensure provided source code does not have any known security issues.
   11. A risk assessment of the application environment, with a documented issues list and plan to address discovered issues on at least an annual basis.
   12. A risk management plan to continually address and remediate discovered issues.
   13. Periodic vulnerability testing of the environment to discover and remediate potential vulnerabilities.
14. A Data Destruction Policy which demonstrates that data no longer in use or required to
    be retained will be destroyed to National Association for Information Destruction (NAID
    – www.naidonline.org) standards.

vii. Provide support for the application(s) running on a defined set of:

1. Operating Systems and supporting system services (e.g., OpenSSH, OpenSSL, Apache,
    Systemd).
2. Relational Database Management System Software (e.g., Oracle, SQL Server, MySQL).
3. Third-party software such as Application Servers, Web Servers, Security Software,
    Support Libraries, and other software required for daily operation of the application(s).

viii. If there are discovered security vulnerabilities in the previously described items and/or the
     application(s), the following need to be provided within 48 hours to IU Health:

1. Mitigation steps that IU Health can undertake to mitigate the reported vulnerabilities.
2. A timeline for any application patches that need to be applied to the environment to
   mitigate vulnerabilities.
3. A timeline for testing and approval of patches to any of the supporting items described
   above.

ix. If there are discovered security vulnerabilities in the previously described items and/or the
    application(s), the following need to be provided within seven (7) days to IU Health:

1. Instructions for patching the supported items to restore the security posture of the
    environment.
2. Instructions for patching the application to restore the security posture of the
    environment.

x. Ensure that the Operating System, any Relational Database Management System Software, and
    Third-Party software is supported by both the system and/or software vendors for the system
    lifecycle with system updates and security patches. If any of these components become
    unsupported, the Provider needs to address this before the system has an unsupported component.

xi. Provide documentation on the organization’s Incident Response Plan, and a current list of
    security contacts for reporting vulnerabilities or compliance issues.

xii. Allow IU Health the right to audit information systems in the scope of the system(s) in scope of
     this Agreement.

xiii. Provide IU Health a data dictionary in ISO 11179 format and instructions on how to extract data
     in a defined industry-standard format (e.g., Text, database backup, etc.) using industry standard
     tools.