Indiana University Health, Inc. Verification and Validation Using Distributed Computing Requirements

These are minimum requirements required by IU Health’s Information Security Program for technologies used on behalf of IU Health to provide verification and validation services utilizing distributed computing. Such technologies include Blockchain, which is its current and most common usage. We recognize that this is a technology that can provide significant benefits to IU Health through their use to validate and verify transactions. The purpose of these requirements is to ensure that the underlying distributed computing technologies utilized on behalf of IU Health are properly assessed and monitored for vulnerabilities that may compromise their integrity, and the data and systems they are meant to provide integrity for. 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 that utilizes distributed computing technologies to provide verification and validation services to ensure the integrity of IU Health data is subject to these requirements. Therefore, any system implemented as part of this agreement must:

i. Demonstrate that no data that can be classified as Protected Health Information (PHI), Payment Card Industry-Data Security Standards (PCI-DSS), Family Educational Rights and Privacy Act (FERPA), or Privacy Act data will be stored as part of these systems.

ii. Demonstrate that only minimum necessary data from source systems is used to generate cryptographic hashes using a SHA-256 or greater hashing algorithm which will be stored on said Distributed Computing Service.

iii. Demonstrate that no single entity will have control of more than 50% of the total computing power available to process transactions for distributed computing services. This is because if one entity has control of more than 50% of the computing power, they will be able to alter transactions and compromise system integrity.

iv. Ensure that all participants in the distributed computing service promptly remediate discovered vulnerabilities in the operating system, applications, cryptographic subsystems, and third-party support software that directly interfaces with it or produces data to be utilized by the service within seven (7) days.

v. Ensure that all participants in the distributed computing service have a security management program in place to cover not only the assets involved in the distributed computing service, but also all other assets in the purview of the organization.

vi. Enforce, utilizing network-based and logical controls, that only authorized parties can read, write, or otherwise access the Distributed Computing services.

vii. Enforce, utilizing network-based, logical, and physical controls, that the assets participating in the distributed computing service are only allowed to connect to systems or services required for authentication, disaster recovery, minimum necessary data interchange, administration, or maintenance.

viii. Enforce, utilizing a combination of network-based and contractual controls, the following security controls and practices to address network-based spoofing and interception attacks, including BGP Hijacking and DNS Hijacking:
   a. Participant(s) will make sure that the internetworking infrastructure hosting distributed computing services in the scope of this agreement have Autonomous Service Numbers (ASNs) registered with the American Registry for Internet Numbers (ARIN – www.arin.net) or the equivalent for their geographic area(s).
   b. Participant(s) will make sure that all networking prefixes advertised by the ASNs for routing are properly registered with ARIN or its equivalent(s).
   c. Participant(s) will make sure that all networking providers that exchange traffic through peering arrangements filter announcements of their registered and advertised network address space by non-registered ASNs.
   d. Participant(s) will make sure that the provider(s) providing the internetworking infrastructure hosting their services have staffed Network Operations Center(s) operating 24 hours a day, 7 days a week.
   e. Participant(s) will make sure that the following service level agreements are in place with their provider(s):
Information Security

i. 5 minute alerting on network failures or issues with Border Gateway Protocol (BGP) or Domain Name Services (DNS).

ii. 30 minute escalation to an on call network engineer who can make changes to Border Gateway Protocol (BGP) policies or DNS configurations in real time.

ix. Allow IU Health and other members of the Distributed Computing services to audit information systems in the scope of the system(s) in scope of this agreement.

x. Allow IU Health and other members/users of the Distributed Computing services to monitor the health of and system connectivity of information systems in the scope of the system(s) in scope of this agreement.

xi. Allow IU Health and other members/users of the Distributed Computing services to monitor the security posture of information systems in the scope of the system(s) in scope of this agreement, including operating system vulnerabilities, application vulnerabilities, network vulnerabilities, and cryptographic system vulnerabilities.

xii. Allow IU Health and other members/users of the Distributed Computing services to terminate all access to any information systems which have not been patched or remediated for vulnerabilities within seven (7) days as they pose a risk to the integrity of the system.

xiii. Provide strong, mutually agreeable, documented, and auditable processes for validating and verifying the identities of all participants in the Distributed Computing system.

xiv. Provide verifiable Public Key Infrastructure digital certificates and identities to identify all participants that are issued by a mutually agreeable third party. Self-signed certificates are not acceptable.

xv. Ensure that all data elements utilized as part of the distributed verification and validation system undergo data quality checks. This is to make sure that we only utilize verified and validated data as inputs.

xvi. Ensure that transactions recorded as part of the distributed verification and validation system can be reconciled against transactions from the source computing resources.

xvii. Ensure that identities used to publish transactions to the distributed verification and validation system can be verified, and the cryptographic identities of the series of transactions said identities made can be validated.

xviii. Demonstrate third-party risk management processes by mapping cryptographically verified identities involved in transactions to legal entities, and identifying and reconciling all legal entities in the transaction chain.

xix. Ensure that there is a documented method and process for appending records to the system to amend existing records in case of a correction.

xx. Ensure that there is a governance process by which disputed transactions can be arbitrated and amendments posted to the distributed verification and validation system.