Information Security

Indiana University Health, Inc. Payment Card Industry – Data Security Standards Requirements

These are minimum requirements required by IU Health's Information Security Program for technologies used on behalf of IU Health for processing payment, credit, or debit cards in accordance with the Payment Card Industry – Data Security Standards (PCI-DSS) set by the PCI Security Standards Council. These are minimum acceptable security standards for protecting this information.

Any information technology system implemented as part of this Agreement that processes, stores, transmits, or receives payment, credit, or debit card information is subject to these requirements. Therefore, any system implemented as part of this agreement must:

i. Demonstrate full compliance with the PCI-DSS standards and associated amendments, available at https://www.pcisecuritystandards.org/ by demonstrating how IU Health will be able to achieve a successful Attestation of Compliance (AOC) by a Qualified Security Assessor (QSA) with the proposed solution.

ii. Work with IU Health to maintain full compliance, verifiable with successful Attestations of Compliance (AOC) with PCI-DSS security standards throughout the product lifecycle by developing an operational management plan to ensure currency of all in-scope components, including operating systems, supporting software, and third-party libraries.

iii. When the PCI-DSS standards update to a new version, provide an operational plan to ensure IU Health's compliance with it before the retirement date of the previous standard.

iv. If any part of the PCI-DSS solution is outsourced, provide the following for review by both the Enterprise Architecture and Information Security teams on an annual basis or upon update of the systems in scope to the current standards version:

   a. A PCI-DSS Attestation of Compliance (AOC) for the current standards version completed by a certified Qualified Security Assessor (QSA). We will not accept self-attestations or any substitute documentation.

      i. We will accept a verified successfully completed AOC in lieu of an IT Risk Assessment (ITRA).

   b. A Service Organizations Control Level 2 (SOC 2) report and HITRUST Common Security Framework (CSF) certification letter or ISO 27001/27018 certification by a certified accountancy for remote or cloud-based hosting facilities.

   c. A data flow diagram showing payment card data flow from entry to ultimate disposition of data.

   d. A network architecture implementation diagram demonstrating required segmentation, firewall rules, and network protection including firewalls, Intrusion Detection Systems/Intrusion Prevention Systems (IDS/IPS), Data Loss Prevention/Cloud Access Security Broker technologies (DLP/CASB), Security Incident and Event Management Event Logging (SIEM), and strong cryptography.

   e. 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.

   f. 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.

   g. Ensure that third parties that provide scripts or services to support the credit card processing environment have sufficient security controls, including PCI-DSS Attestation of Compliance where appropriate, to prevent malicious hijacking of their scripts. This is to help prevent Magecart-type attacks where credit card data is sent not only to its legitimate destination, but also to malicious third parties.

   h. 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.

   i. Demonstrated two-factor authentication for administrative system access utilizing system(s) compliant with the NIST Special Publication 800-63B standards.

   j. Demonstrated provisioning and identity validation/proofing processes that are compliant with NIST Special Publication 800-63B standards.

   k. If the Business Associate or Third Party will not be compliant with the above, a documented explanation must be provided in a timely manner along with associated risk mitigation strategies.

v. If the PCI-DSS solution involves the collection of credit, debit, or payment card data over phone or voice telecommunication services, the standards in the PCI Standards Security Council Information Supplement, Protecting Telephone-Based Payment Card Data, must be followed for the most current version of the document available.
   a. The solution must be validated and certified by a certified QSA before production operations.

vi. Ensure that all in-scope devices promptly remediate discovered vulnerabilities in the operating system, applications, cryptographic subsystems, and third-party support software within seven (7) days.

vii. Enforce, utilizing network-based and logical controls, that only authorized parties can read, write, or otherwise access PCI-DSS data.

viii. Actively block traffic from malicious sources identified by the Financial Services Information Sharing and Advisory Center (FS-ISAC) and its member institutions.

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

x. 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):
      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.

xi. Allow IU Health to audit information systems in the scope of the system(s) in scope of this agreement, including mutually agreed-upon penetration tests and vulnerability scans by the IU Health Information Security team or a certified Qualified Security Assessor.

xii. Allow IU Health to monitor the health of and system connectivity of information systems in the scope of the system(s) in scope of this agreement.

xiii. Allow IU Health 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.

xiv. Provide strong, mutually agreeable, documented, and auditable processes for provisioning, validating, and verifying the identities of all parties with access to PCI-DSS data in accordance with NIST Special Publication 800-63B standards.

xv. Destroy all data no longer in use or required to be retained using a National Association for Information Destruction (NAID – www.naidonline.org) certified provider for PCI-DSS data.