Indiana University Health

Information Security

Indiana University Health, Inc. Wireless, Cellular, Real Time Location System (RTLS), Radio Frequency Identification (RFID), and Near Field Communications (NFC) Requirements

These are minimum requirements required by IU Health's Information Security Program for technologies used on behalf of IU Health for the implementation or usage of Real Time Location Systems (RTLS), Radio Frequency Identifier (RFID), or Near Field Communication (NFC) systems. As these technologies have the potential to be used to support patient tracking, supply chain operations, patient engagement, and tracking of equipment and assets, IU Health needs to ensure that the data and algorithms used by these systems is demonstrably accurate and protected.

Any information technology system implemented as part of this Agreement that implements these technologies is subject to these requirements. Therefore, any system implemented as part of this agreement must:

i. Define exactly what use cases the solution(s) will be utilized for in the IU Health environment.
ii. Ensure that this system will not store Protected Health Information (PHI), Personally Identifiable Information (PII), Payment Card Industry-Data Security Standards (PCI-DSS), or Family Educational Rights and Privacy Act (FERPA) data.
    a. Payment Solutions that utilize Near Field Communications, such as Apple Pay, are covered by the PCI-DSS security requirements and are exempt from these requirements.
iii. Only utilize minimum necessary data to achieve the desired use cases.
iv. Use system-generated numbers or identifiers that are not based on PHI, PII, PCI-DSS, or FERPA data.
v. Utilize mapping and location information supplied by Design & Construction and Telecommunications.
vi. Ensure that there is adequate wireless coverage for the areas and defined use cases for successful operation of the solution.
vii. Ensure that there is no interference with existing wireless solutions.
viii. Whenever possible, provide enclosures or mechanisms to reduce the potential for signal interception.
ix. Follow cabling and installation standards as defined by the IU Health Telecommunications team in their standards documentation.
x. Systems must be able to be segmented from the main corporate network and communicate over a defined set of network addresses, ports, and protocols to a defined set of IP addresses.
xi. Systems used to send and receive collected data and transmit/receive said data to and from official systems of record, including Enterprise Resource Planning (ERP), Electronic Medical Record (EMR) systems, or other designated IU Health applications, must run vendor-supported operating systems, databases, and supporting libraries, and be patched against known vulnerabilities.
xii. If the solution contains Bluetooth 4.0 or greater or Bluetooth Low Energy (LE):
    a. Security Levels 2, 3, or 4 must be enabled using at least 128-bit Advanced Encryption Standard (AES-128) and Elliptic Curve Diffie-Hellman Key Exchange (ECDHE).
    b. Bluetooth LE Privacy Mode must be enabled to prevent eavesdropping of individual Media Access Control (MAC) addresses.
xiii. If the solution utilizes Near Field Communications (NFC):
    a. Change the encryption keys from the default settings.
    b. Follow the security standards in the ECMA-385 standard, NFC-SEC-NFCIP-1 Security Services and Protocol.
xiv. If the solution supports Wireless Internet utilizing Wi-Fi:
    a. Support the latest standards that IU Health supports.
    b. Support WPA2 or WPA3 authentication to encrypt data in transit and protect against improper alteration of data.
xv. If the solution supports cellular technologies, either Long Term Evolution (LTE/4G) or IMT-2020 (5G):
    a. Solution must be deployed using 5G network slicing to isolate application traffic to a defined segment if using direct device connectivity whenever possible.

b. If the solution utilizes site to site connectivity, Software Defined Wide Area Networking (SD-WAN) technologies must be used to protect communications.

c. All transit utilizing LTE or 5G networks must be actively monitored for security events.

d. 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.

e. 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.

f. Periodic vulnerability testing of the environment to discover and remediate potential vulnerabilities.

g. All equipment utilized in the transit of data from the access points to the termination point at the IU Health network must be kept current and protected against security vulnerabilities.

  i. Any equipment utilized in the transit of data must not be from a prohibited vendor covered under Section 889 of the National Defense Authorization Act (NDAA) of 2019.

h. 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:

  i. 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).

  ii. Participant(s) will make sure that all networking prefixes advertised by the ASNs for routing are properly registered with ARIN or its equivalent(s).

  iii. 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.

  iv. 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.

  v. Participant(s) will make sure that the following service level agreements are in place with their provider(s):

    1. 5 minute alerting on network failures or issues with Border Gateway Protocol (BGP) or Domain Name Services (DNS).

    2. 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.

xvi. Provide a monitoring system, model processes, and support in detecting the following fraudulent usage scenarios:

a. Unauthorized tag or device cloning.

b. Multiple instances of tag or device IDs.

c. Unauthorized alteration of stored values on devices or tags.

xvii. Provide structured asset management data on all devices or tags that can be imported into an enterprise asset management system, including but not exclusive to:

a. Serial Number

b. Device Name

c. Device Type

d. Media Access Control (MAC) Addresses

e. Firmware Version.

f. Date of Manufacture.

g. Warranty Dates.