**Hosp.id.ality IoT Wristband**

Team 1: Josue Camejo, Manuel Hernandez, Melanie Maestre, Michael Soto, David Salmeron, Theodore Atis

CNT4182: Mobile & IoT Cybersecurity

Professor Dr. Charlyne Walker

July 16, 2023

Table of Contents

[Project Hosp.ID.ality 2](#_Toc140603155)

[Overview 2](#_Toc140603156)

[Goals 2](#_Toc140603157)

[Specifications 2](#_Toc140603158)

[Stakeholders 3](#_Toc140603159)

[Primary Users 3](#_Toc140603160)

[Secondary Users 3](#_Toc140603161)

[Features 3](#_Toc140603162)

[Data Flow  5](#_Toc140603163)

[Enhancements 6](#_Toc140603164)

[Processing 6](#_Toc140603165)

[Input Data 7](#_Toc140603166)

[Access to Data/Privileges 8](#_Toc140603167)

[Analytics in the Cloud 9](#_Toc140603168)

[Communication protocols used for interconnectivity 11](#_Toc140603169)

[Cloud services platform 12](#_Toc140603170)

[Mobile device software 14](#_Toc140603171)

[Mobile OS and supported form factors 15](#_Toc140603172)

[Monetization 15](#_Toc140603173)

[Time-Based Monetization 16](#_Toc140603174)

[Production Costs 16](#_Toc140603175)

[Cost Breakdown of Hardware/Software 17](#_Toc140603176)

[Two-Year Projection Breakdown for Hypothetical Customers 18](#_Toc140603177)

[Application Program Interface (API’s) 18](#_Toc140603178)

[Risk Assessment and Mitigation 20](#_Toc140603179)

[Mitigation & Controls 22](#_Toc140603180)

[NFC Communication Vulnerabilities 23](#_Toc140603181)

[Appendix A 27](#_Toc140603182)

[Incident Response Plan (IRP) 28](#_Toc140603183)

[Appendix B 35](#_Toc140603184)

[Privacy Impact Assessment 36](#_Toc140603185)

# Project Hosp.ID.ality

## Overview

The “Hosp.id.ality” product will help Healthcare workers and staff be able to quickly authenticate their identity and gain the necessary access whether physical or access to a digital whiteboard. By utilizing Near-field Communication (NFC) technology, the users would tap the readers/integrated technology in the respective rooms and make updates where necessary.

## Goals

Enhance patient safety by providing real-time tracking, ensuring that patients are in their assigned rooms or designated areas. This minimizes the risk of patient wandering or getting lost, allowing for timely interventions, and reducing the chances of accidents or adverse events. Secondly, it improves efficiency and workflow by enabling healthcare staff to quickly locate patients, saving valuable time, and streamlining care delivery. Visiting medical personnel can efficiently locate patients they need to attend to, optimizing their schedules and ensuring timely consultations or treatments. Additionally, designated family members can have peace of mind knowing the whereabouts of their loved ones and can plan their visits accordingly.

The mobile IoT device improves patient safety, enhances operational efficiency, and provides convenience to all stakeholders involved in patient care.

## Specifications

In hospitals around the country, the use of Radio-Frequency Identification (RFID) technology has been implemented to keep track of numerous things. From tracking medications and supplies to personnel that are entering the facilities. There is a concern of security and integrity since anybody who can gain physical access to the facility can become a serious threat. Some more potential benefits from having more data to process would be insight on employee efficiency/performance. Scanning the wristband and updating the whiteboard would also help keep track of inventory and where it is being distributed amongst the Healthcare networks. By service providers (i.e., doctors, nurses, doctor’s assistants, etc.) utilizing this technology, there would be improved security and risk mitigation as opposed to using a whiteboard with no security past the main entrance of these facilities. Through the hardening of these systems, there could possibly be fewer financial burdens incurred from disputes like injury torts and negligence lawsuits.

# Stakeholders

## Primary Users

**Hospital Staff**: This product would be used extensively by hospital staff, including nurses, doctors, and administrators. They would utilize the device and associated software to monitor patient locations, ensure patients are in their assigned rooms when needed, and efficiently allocate resources based on real-time information. Administrators, managers, and supervisors within the hospital can utilize the tracking data for operational purposes. They can analyze patient flow patterns, identify bottlenecks, and make informed decisions to improve efficiency and resource allocation within the hospital.

**Visiting Medical Personnel**: Doctors, therapists, specialists, and other visiting medical personnel who provide care and treatment to patients in the hospital would also benefit from this product. They can easily locate patients they need to see, track their movements for timely interventions, and optimize their time management.

**Designated Family Members**: Families of the patients play a vital role in their care and well-being. Providing designated family members with access to the tracking information can help alleviate their concerns and keep them informed about the patient's location, especially during procedures, tests, or therapy sessions.

## Secondary Users

**Hospital Security Personnel**: Security personnel can benefit from the tracking information to enhance the safety and security of patients, staff, and hospital premises by monitoring patient movements and identifying any unusual activities or security breaches.

**Law Enforcement**: Law enforcement agencies may occasionally interact with hospitals in specific situations, such as investigations or emergency responses, their involvement in patient location tracking would be limited and subjected to legal and privacy considerations.

**Interpreter/ Translator**: In the context of patient location tracking, interpreters may utilize the device and associated software to locate patients they are assigned to assist. By having access to real-time patient location information, interpreters can efficiently navigate the hospital facility and reach the patients they need to support, ensuring timely and effective interpretation services.

**Insurance Claim Adjusters**: In some cases, insurance companies may require information about the location and movements of patients in hospitals to assess insurance claims or verify the validity of treatments or procedures. Claim adjusters may utilize the device and associated data to validate the accuracy of the information provided by the policyholder or the hospital.

**Paramedics**: Ambulance paramedics can highly benefit from having this sense it can track the vital signs from the ambulance to the hospital. This can work not just for the paramedics, but also for the law enforcement who are escorting the individual to the hospital to check on the vital signs and what changes have occurred since the time he or she has been in the ambulance.

# Features

**Real-Time Location Tracking:** The device would provide real-time tracking of patient locations within the hospital premises, allowing users to monitor their movements and whereabouts. This would be a layer 5 application as the tracking would be a third-party cloud software working with the product(s).

**IPS (Indoor Positioning System):** The device would utilize IPS technology, such as Bluetooth Low Energy (BLE), Wi-Fi, or Ultra-Wideband (UWB). This would allow for accurate tracking. Also, this feature operates on the Layer 3 section of the IoT stack as it has to do with communication between devices or better known as connectivity. (BOTH backend and Customer-based requirement).

**Patient Identification:** The device could incorporate patient identification features, such as unique identifiers or barcode scanning, to ensure accurate association of location data specific to patients. This would have to do with Layer 1 as the device would have communicating hardware to identify itself and the users’ credentials saved to the wristband. (BOTH backend and Customer-based requirement).

**Mobile Connectivity:** The device would have connectivity options such as Bluetooth or cellular connectivity to transmit location data to a central server or cloud-based system in real-time. Implementing this feature would be situated on Layer 3 as it is communication between devices and/or servers. (BOTH backend and Customer-based requirement).

**User-Friendly Interface:** The device may have a simple and intuitive user interface, such as an LCD screen or LED indicators, to display location information or provide feedback to the user. Layer 1 would have to do with this feature as the physical hardware like an interface or even LED indicator would be additional hardware added to the device. (Customer-based requirement)

**Data collection:** Reporting errors will stream to the Cloud. Errors such as connectivity errors, and unrecognized inputs will be collected as analytics information and sent to the Cloud. This is considered a Layer 4 feature.

**Remote Updates:** Embedding software within the IoT device to ensure remote updates can initiate through cloud communication is considered a Layer 2 feature.

**Data Encryption and Security:** Patient location data transmitted or stored by the device should be encrypted to ensure data security and privacy, complying with healthcare data regulations and protocols. This would suit Layer 3 since it has to do with encryption within communication protocols that are nested within Layer 3. (BOTH backend and customer-based requirement)

A close-up of a sign

Description automatically generated

# Data Flow A picture containing text, screenshot, diagram, design Description automatically generated

The device will pass data from the hardware layer up the stack to ensure patient identification (barcode scanning, unique ID codes) are signaled up to the cloud platform, and cloud applications for logging. Remote updates would travel down the IoT layers from the Cloud Application Layer to the Device Software Layer, as the update would initiate from an automated cloud server and could become an enabled manual process in the device application. The data passed through the stack is encrypted. The diagram below details the user requirement data flow chart.

# Enhancements

The feature or functionality that requires or is enhanced by the data element is the "Real-Time Location Tracking" feature. This feature relies on the data element of patient location information to provide real-time tracking of patients within the hospital premises. By monitoring their movements and whereabouts, it enables healthcare staff, visiting medical personnel, designated family members, and other stakeholders to efficiently locate patients, ensure they are in their assigned rooms, and optimize care delivery. This real-time tracking data is crucial for achieving the goals of enhancing patient safety, improving efficiency, and streamlining care delivery.

## Processing

The data will be collected and processed on the device. The device will have the capability to report errors, such as connectivity errors and unrecognized inputs, which will be collected as analytics information and sent to the cloud. This indicates that data processing will occur on the device to identify and report such errors.

Additionally, features like patient identification and user-friendly interface indicate that the device will process and utilize patient-specific data for identification purposes and display relevant information to users. It’s important to note that while some data processing will occur on the device, there will also be data transmission and processing occurring on cloud-based systems or servers. Features like remote updates, data encryption, and security indicate that certain data processing tasks, such as software updates and encryption of patient location data, will be performed in the cloud or backend systems associated with the device.

A picture containing text, screenshot, font, white

Description automatically generated

# Input Data

The required input data for the system will be supplied by the following stakeholders:

**Hospital Staff:**

Hospital staff, including nurses, physicians, and administrators, will play a crucial role in supplying input data. They will be responsible for updating patient locations and making necessary updates through the device’s interface. Their motivation to supply the data arises from the need to enhance patient safety, improve workflow efficiency, and allocate resources effectively within the hospital.

**Visiting Medical Personnel:**

Visiting medical personnel, such as physicians, therapists, and specialists, who provide care and treatment to patients in the hospital, will also need to supply input data. They will utilize the system to locate specific patients they need to see and track their movements for timely interventions. Their motivation to supply data stems from the desire to optimize their time management, ensure timely consultations or treatments, and contribute to efficient care delivery.

**Designated Family Members:**

Designated family members of patients will have access to tracking information about their loved ones. While they may not directly supply input data, their motivation to ensure that data is supplied lies in having peace of mind and being informed about the whereabouts of the patient. This information allows them to plan their visits accordingly and feel reassured about the patient’s location during procedures, tests, or therapy sessions.

It’s important to note that other stakeholders, such as hospital security personnel, law enforcement, interpreters/translators, insurance claim adjusters, and paramedics, may have limited involvement in supplying input data for patient location tracking. Their motivation would vary based on their specific roles and responsibilities within the healthcare ecosystem.

Through the hospital staff updating these systems through the interface in a timely manner, it would be indicative of employee efficiency. Through an increased throughput on employee efficiency there could be possible incentives like bonuses, raised wages, etc. for employees that are continuously improving.

# Access to Data/Privileges

**Hospital Staff**: Hospital staff, including physicians, nurses, and administrators, can have access to real-time tracking of patient data. The goal is to monitor patient movement, optimize resource allocation, and improve operational efficiency in hospitals.

**Security Personnel**: Hospital security personnel may have access to track patient data and other security activities. Its purpose is to ensure the safety of patients, staff and hospital facilities by monitoring patient movements and detecting suspicious activity or breaches of security.

**Administrators and Managers**: Hospital administrators and managers can have access to track patient data historically. The goal is to analyze patient flow patterns, identify bottlenecks, and make decisions based on historical data to improve operational efficiency and resource allocation.

**Designated Family Members**: The displayed patient's family can be granted access to track real-time patient data. The goal is to provide information to the family about the patient's location, especially while a procedure, test, or therapy session is taking place.

**Law Enforcement (where appropriate):** Law enforcement may have limited access to patient data in certain situations, such as in a crime investigation or emergency response. Their access will be subject to applicable legal and privacy considerations.

**Analytics**

Analytics can be performed either at the edge, in the cloud, or both, depending on your specific needs and circumstances. Here is an explanation and justification for each choice:

**Analytics on the Edge**:

Low Latency: By performing analytics at the edge, data can be processed and analyzed right where it came from without sending it to the cloud first. This reduces time latency, which is important for applications that require fast response times, such as in critical situations or real-time decision making.

Security and Privacy: In some cases, sensitive data may be better processed and analyzed at the edge to maintain security and privacy. By reducing the transfer of data to the cloud, the risk of exploitation or security breaches can be reduced.

Dependence on Internet Connection: Analytics at the edge allows data processing to occur locally, not requiring a stable internet connection. This is useful in environments with limited networks or in remote locations.

# Analytics in the Cloud

**Scalability and Capacity**: Cloud computing provides unlimited computing resources and high scalability. Analytics in the cloud enable processing of complex and large data at high speed and can manage large volumes of data with ease.

**Collaboration and Access**: Analytics in the cloud enables easy access and collaboration between different users or departments. Data can be accessed from multiple locations, facilitating team collaboration and consistent data access.

**Combination of Analytics on Edge and Cloud:**

**Hybrid Approach**: This option combines the advantages of analytics at the edge and in the cloud. Data can be processed and analyzed at the edge for real-time decisions, while data that is more complex or requires deeper analysis can be sent to the cloud for more sophisticated, end-to-end analytics.

**Cost Savings**: By adopting a hybrid approach, cloud usage can be optimized by selecting data to be processed in the cloud, reducing data transfer costs, and using cloud resources efficiently.

The choice between analytics at the edge, in the cloud, or both depends on application requirements, response speed required, desired complexity of analytics, data security, and resource availability. A hybrid approach can provide flexibility and balance between response speed, capacity, and cost savings.

**Predictive Analytics**

The user will be able to identify his or her heart rate as well as information regarding blood pressure, sugar level, and heart rate. It will also state the user's name just with an ID number which will make it easier for faculty to identify the user as well as which nurse, they are assigned to. The wristband will also notify the user when it's time for them to take their medication so that they can notify the nurse. It will achieve this counting down to the last time the user took their medication. One last thing that the user can benefit from is the use of messages since the wrist band allows them to send and receive messages from the user's family if the user has it paired up with their phone.

**Who should have access to the data (both real-time and historical) and why?**

The user should have access to their own real-time data, and historical data at their request to ensure accurate reporting, and to comply with standards. Identity access managers and administrators should have access to the data to ensure the deprovisioning and provisioning of user access is facilitated. Employed health personnel with the need to know should have access to the real-time and historical data of the patient’s location information for clinical documentation.

**Sensor devices** (*Adafruit Industries 360 NFC/RFID Transponders*):

Below is some information on the sensors and equipment that is being proposed for this project. The AdaFruit Industries 360 <https://www.arrow.com/en/products/360/adafruit-industries>) is a small quarter-sized chip that has 1 KB of non-volatile storage; it has built in encryption. It communicates to a maximum of 2” which can minimize listening to frequencies. It functions by utilizing most NFC/RFID reading/writing software. This sensor would be the cost-effective device hardware utilized in the wristbands to communicate with the mobile applications that would integrate all of the information being updated.

**Gateway devices** ([IGN500 Ignition MQTT Edge Gateway | OnLogic](https://www.onlogic.com/ign500/?msclkid=a7fc87324f5b162408f7e3bfba3d8ffb&utm_source=bing&utm_medium=cpc&utm_campaign=US-Search%20-DSA-%20Partners&utm_term=ign5&utm_content=Ignition))

Cisco describes a gateway device as “a device [or node] that connects disparate networks by translating communications from one protocol to another.” It is becoming commonplace to utilize routers as gateway devices, albeit their original devices were separate. According to Cisco’s webpage comparing routers with gateway devices, SOHO (small office home offices) now use Wi-Fi routers as both “router (delivering data) and a gateway (translating it so destination devices can use it).” The basic function of a network gateway device includes NICs, I/O, and specialized software to enable translation of network protocols. Gateways may also have additional software for functions, remote adjustments, and deployment controls. Gateway devices operate on the network layer and can operate on all seven layers of the OSI model. The gateway devices can also be used as firewalls to scan and filter data, and for other security purposes. The gateway device for this project is the Ignition MQTT Edge Gateway which translates the MQTT protocol for IoT devices.

The MQTT broker can communicate to the Azure instances via port 8883 via TLS. In such cases where physical devices are installed as gateway devices, or for firewall purposes, the installation should remain loyal to the hospital. To remain compliant with HIPAA (Health Insurance Portability and Accountability Act), firewalls/routers within health services should enable logging relevant with patient data. The physical gateways should essentially operate similarly to routers, and the software to monitor the gateways should enable communication, and monitoring, and provide overview into MQTT protocol transmission.

Another useful tool to implement is the MQTT broker cloud service that offers monitoring, and oversight into the network data. ([EMQX Cloud: Fully Managed MQTT Service for IoT](https://www.emqx.com/en/cloud))

# Communication protocols used for interconnectivity

For device to device and cloud communication, the following protocols would be used. Message Queuing Telemetry Transport (MQTT) to broadcast message updates to the MQTT-Broker which will in turn communicate with the Microsoft Azure instances. DICOM, also known as Digital Imaging and Communications in Medicine, can be used for transmitting, storing, and sharing medical images and related information. FHIR also known as Fast Healthcare Interoperability Resources is used for exchanging healthcare data. It uses web-based APIs and supports a wide range of data types, making it suitable for exchange of data between different healthcare systems. Rather than relying on local servers we utilize the cloud to provide efficient connection as well as more workload and layers of security. It also works well with syncing data like storage. Unlike local storage that can only be accessed from office areas and cloud storage from the device can be accessed anywhere.

# Cloud services platform

The services utilized for this project would be Microsoft Azure's enterprise grade tools. Azure provides various services for IoT applications, including Azure IoT Hub, IoT Edge, Event Hubs, Functions, Cosmos DB, and Azure Blob Storage. Azure IoT Hub enables secure devices connectivity and communication, while Azure IoT Edge allows for edge computing Capabilities: Azure Event Hubs can handle high-throughput ingestion of telemetry data from the IoT devices. Azure Functions can be used to execute serverless code for data processing or triggering actions based on incoming data. Azure Cosmos DB can serve as a globally distributed and scalable database for storing patient location information. Azure Blob Storage can be utilized for storing and retrieving data files, such as device firmware or patient records.

We believe that Microsoft Azure can provide a robust and scalable infrastructure for our product. It offers comprehensive IoT integration, real-time data processing, storage options, serverless computing, etc. This enables our team to build a powerful and intelligent solution to enhance patient care and optimize hospital operations.

**Analytic software**

The analytical software to be utilized also comes from Microsoft’s cloud services. Azure Stream Analytics can be used to perform real-time analytics on the streaming data generated by the IoT device. It allows implementation of SQL-like queries to the data stream. This enables the ability to filter, aggregate, and analyze the data in real-time. In addition, Power BI can be also implemented. Power BI by Microsoft is an intelligence tool that can be used to create interactive dashboards and reports. It can connect to various data sources, including Azure services. It can provide visualization like charts, graphs to represent the analyzed data.

The analytics that would be provided to the employees would be information like patient location (room number, floor number), patient information like allergies, vitals, etc. For the family members in the same room that are curious about information about their family member they would be able to see a form that shows what they have scheduled on a digital board integrated with Microsoft Power BI showcasing the minimal user view of the information. Below is a representation on how the different stakeholders/end users would be categorized and their level of privileged access.

**Hospital Staff**

The hospital staff, which includes doctors, nurses, administrators, and support personnel. Would interact with the systems to access real-time data, receive notifications, and utilize the analytics to improve patient care, operational efficiency, and resource management. For instance, doctors and nurses can monitor patient vital signs, track patient locations, receive alerts, and access predictive analytics to make informed medical decisions. Administrators can use the system to analyze resource utilization, occupancy rates, and other key metrics for optimizing hospital operations.

**Visiting Medical Personnel**

Visiting medical personnel like surgeons, physicians, therapists, would be able to see information like patient vitals, room number, floor number, and would be pinged the updates on patient condition like if they have been administered anesthetics or specific conditions relative to the visiting medical professional’s needs.

**Law Enforcement**

Law enforcement officials that would need the information of a patient would be able to see information on the patient's room and floor number.

**Insurance Claim Adjusters**

Insurance Claim Adjusters would be able to see the minimal patient information just like Law enforcement and be shown patient room and floor number.

**Paramedics**

Paramedics would also see this information such as the patient's vitals, blood pressure, calcium level and overall health. The information would also be updated to the hospital once the patient has arrived.

# Mobile device software

**Azure App Service**: Azure App Service will allow us to host our mobile backend as a service (MBaaS) in the cloud. We will create RESTful APIs or deploy server-side logic using Azure Functions or Azure Logic Apps. The mobile software will then communicate with the backend APIs to send or retrieve data, perform business logic, or trigger specific actions.

**Azure Mobile Apps**: We will use Azure Mobile Apps platform-as-a-service (PaaS) to provide a scalable backend for mobile app development. It will provide features like authentication, push notifications, offline data sync, and data storage. Our Mobile software can interact with Azure Mobile Apps to authenticate users, store, and retrieve data, and leverage other backend functionalities.

**Azure Notification Hubs**: To send push notifications from our mobile software, Azure Notification Hubs will be used. It will provide a scalable and cross-platform push notification infrastructure. Our mobile software can communicate with Azure Notification Hubs to register devices, send targeted notifications, and handle push notification responses.

**Azure API Management**: Azure API Management will create, secure, and manage APIs that can be consumed by our mobile software. It will provide features like API versioning, security, rate limiting, and analytics. Our mobile software will communicate with Azure API Management to discover and consume APIs securely and efficiently.

**Azure Event Grid**: Azure Event Grid will enable event-based communication between different Azure services and external systems. Our mobile software will publish events to Azure Event Grid and will configure various event handlers to process those events in real-time or trigger downstream actions.

**Azure Service Bus**: Azure Service Bus will be used as a messaging service that will enable reliable communication between different components and systems. Our mobile software will communicate with Azure Service Bus to send and receive messages, enabling asynchronous communication patterns and decoupling of components. Communication and transfer of data within the device software is based on cloud networking protocol. The device's development software will enhance network-wide information transfer between primary and secondary users.

# Mobile OS and supported form factors

Apple’s iOS, and Android systems will be the main supported mobile operating systems. They will be supported throughout the entirety of the lifecycle of the Hosp.ID.ality because they are the two largest operating systems on the market. The form factors in consideration are phones. For security reasons, the use of tables or their related software could bring about potential security vulnerabilities. Utilizing company phone devices to update database information would prove an effective way to mitigate employees accidentally utilizing personal property and potentially introducing malware.

## Monetization

For customers interested in the Hosp.ID.ality technology, there would be a one-time fee for the wristbands, and initial set up/integration of the cloud technologies. By implementing a licensing or perpetual model, customers will be able to use our product indefinitely for an upfront fee. Additional charges may apply for updates, maintenance, or support. After everything has been set up, there will be a total of three free lifetime service calls. Beyond the three complimentary calls, there would be a higher monthly fee that would provide 24/7 around the clock service calls.

Product demos will be used to demonstrate the value of our product to potential customers. Interactive demonstrations or trials will be conducted to showcase the key features and benefits of Hosp.ID.ality. This allows the customers to experience its value firsthand and understand how it can address their specific needs.

The ways that the product's value can be shown to potential customers without statistics from other customers, would be to conduct research and compare it against the run-time compilation of other systems that are used. Most commonly these groups that handle database management are understaffed since most of the funding is used for healthcare workers, equipment, and medical supplies. Reducing oversight and providing a 5-year cost breakdown analysis of the average savings provided utilizing our systems and the efficiency would be a great way to show potential customers the benefits and value of Hosp.ID.ality.

The end users (hospital staff, authorities, security, etc.) would not be subject to any fees. We will implement customer organization charges where the pricing structure will vary based on the frequency of charges incurred by customer organizations. This could be on a monthly, quarterly, or yearly basis, or linked to specific usage milestones.

## Time-Based Monetization

Initial setup such as software installation to company devices, and system integration would require a one-time fee. Remote software maintenanceduring normal business hours would be charged per use, as clients should have personnel capable of conducting said updates. Physical software maintenance during normal business hours would be charged per use, as clients should have personnel capable of conducting said updates. Both of these maintenance services include security and bug patches free of charge.

Remote support during normal business hours would be based under a monthly subscription fee. Same goes for On-Site Support, during normal business hours. Any support or maintenance required outside of normal business operating hours will be charged on a per use basis.

# Production Costs

Device costs

NFC readers, writers, NFC wristbands vary in the marketplace price ranges. Desco Industries provides a wristband at a cost-effective price for $1.14/unit. Other custom-made NFC wristbands require custom quote requests.

Service Costs

<https://azure.microsoft.com/en-us/pricing/details/cloud-services/>

The potential costs of this service include costs for hosting data in cloud servers and will also include the costs for the mobile Platform as a Service, and the EMQX MQTT broker software.

# Cost Breakdown of Hardware/Software

|  |  |  |  |
| --- | --- | --- | --- |
| **Hardware** | **Cost of hardware** | **Software services** | **Cost of software** |
| **Gateway devices** ([IGN500 Ignition MQTT Edge Gateway | OnLogic](https://www.onlogic.com/ign500/?msclkid=a7fc87324f5b162408f7e3bfba3d8ffb&utm_source=bing&utm_medium=cpc&utm_campaign=US-Search%20-DSA-%20Partners&utm_term=ign5&utm_content=Ignition)) | $853.00 | MQTT EMQX  (Serverless tier) | $3.99 (per hour) |
| **Sensor devices** (*Adafruit Industries 360 NFC/RFID Transponders)* | $2.50 | Azure Blob Storage | $0.15 (per hour) |
| **Wristbands**  *(Desco Industries Wristband)* | $1.14 | Azure Mobile PaaS  (Premium) | $0.40(per wristband) |

# Two-Year Projection Breakdown for Hypothetical Customers

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Price Chart | Annual Premium | Biennial Premium | Standard Annual | Standard Biennial |
| Remote/Onsite support 24 hours | $600,000.00 | $1,200,000.00 | **-Not Included-** | **-Not Included-** |
| Basic customer support during business hours (8am-4pm EST) | **-Included-** | **-Included-** | $192,000.00 | $384,000.00 |
| 4,999 or less users | $10,000.00 | **-N/A-** | $30,000.00 | $60,000.00 |
| 8,000 users or less | $15,000.00 | **-N/A-** | $35,000.00 | $70,000.00 |
| Each additional 2,000 users after 8,000 users | $2,000 per 2,000 users | $4,000.00 | $8,000.00 | $16,000.00 |
| Total Cost | $627,000.00 | $1,204,000.00 | $265,000.00 | $530,000.00 |

## Application Program Interface (API’s)

Azure Storage API will store and retrieve data in a scalable and secure manner. Azure Active Directory (Azure AD) API will provide authentication and authorization services, enabling secure access control to our product. It will allow Hosp.ID.ality to manage identities, roles, and permissions. Azure Resource Manager API will enable programmatic management of Azure resources. It will allow Hosp.ID.ality to automate the provisioning, deployment, and management of its infrastructure.

Although existing APIs will be used, development of custom APIs will be needed to meet specific requirements such as integration with third-party services. This will give Hosp.ID.ality the ability to facilitate seamless integration with external systems or services, allowing data exchange or triggering specific actions. Implementation of real-time data streaming is also a much-needed requirement to enable real-time data streaming between Hosp.ID.ality and other components or applications, ensuring timely and efficient communication. The development of an analytical and reporting API will need to be developed to provide access to analytical data or generate reports based on the data captured by Hosp.ID.ality, allowing users to gain insights and make informed decisions. Our custom-built APIs will be open source to encourage collaboration, community contributions, and foster a developer ecosystem around Hosp.ID.ality.

There are a number of existing Application Program Interfaces (API’s) that can be integrated into the system based on the customers’ needs. API’s function as a bridge between the software application and the database. Microsoft has an API Management system that helps build these interfaces based on the user’s needs. Microsoft also provides inside of the management system the ability to be able to monitor, secure, and manage all facets of the API’s. In the event the customer would like a less customized and more cost-effective solution, International Business Machines (IBM) has a great API that integrates databases into cloud environments to better communicate with the cloud instances we would install for the customers. IBM’s cloud database API (Version 5) functions through a REST API and is able to be written in three modern languages that are commonly used; Node.js, Go(lang), and Python.

# Risk Assessment and Mitigation

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **Negligible** | **Minor** | **Moderate** | **Significant** | **Severe** |
| **Very Likely** | Low | Moderate | High | High | **Unauthorized access to an employee wristband** |
| **Likely** | Low | Moderate | Moderate | High | High |
| **Possible** | Low | Low | **Supply Chain Attack** | Moderate | High |
| **Unlikely** | Low | Low | **Data Corruption** | Moderate | Moderate |
| **Very Unlikely** | **RFID skimming** | Low | Low | Moderate | Moderate |
| Risk Matrix | | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threat** | **Vulnerability** | **Asset and Consequences** | **Risk** | **Solution**  **(Deterrence/Detection)** |
| Unauthorized access to an employee wristband | Gain undetected access to databases and other systems. | Databases, software, employee/patient information. | High  HIPAA violation.  ($100-$50,000 per violation) | Multi-Factor Authentication (MFA) when a user wants to update the database. Frequent employee training and awareness programs. MQTT security measures to protect data in transit. |
| RFID skimming | View information in transit. Possibly executing a man in the middle (MITM) attack/ Session jacking. | Wristband credentials, IP addresses of cloud servers. | Low  Network port scans slowing down operations. | Disable all RFID frequencies from wristband, only utilize the NFC frequency grouping(s). |
| Supply Chain Attack | Reverse engineer vendor’s NFC product and attempt various attacks. | Physical hardware including the RFID/NFC chip inside wristbands. | Moderate  Replacement costs of RFID/NFC chips. | Push updates from vendors within a timely manner, actively threat hunt. |
| Data Corruption | Able to interfere with signal corrupting data in transit and potential Denial of Service attack (DOS). | Cloud servers, API’s potentially being knocked offline from corrupted data forcing a reboot sequence. | Moderate  Downtime of operations, cost of services being down, outages affecting employee efficiency. | Push updates, verify power utilized isn’t larger than power when transmitting to verify data corruption is not occurring. |

## Mitigation & Controls

MQTT presents a handful of vulnerabilities which could lead to DDoS, and man-in-the-middle attacks. By default, MQTT implementations do not all have encryption nor authentication, which often leads to reports of higher risk and vulnerabilities such as man-in-the-middle attacks reported by Kaspersky. However, the control for this potential vulnerability is the transport layer encryption through TLS. [Tracking your heartbeat…and payment data? 33 vulnerabilities found in the data transfer protocol for wearable devices | Kaspersky](https://www.kaspersky.com/about/press-releases/2022_tracking-your-heartbeatand-payment-data-33-vulnerabilities-found-in-the-data-transfer-protocol-for-wearable-devices)

Mitigation and remediations could be applied to these vulnerabilities as identified in Orchestrating and Automating Security for the Internet of Things (Cisco 2018) MQTT security “can be divided into three layers”, network, transport, application; these layers are addressed as avenues of defense. Network layer protections include VPN, or a physically secured connection. Alternative ways to ensure secure communications between MQTT endpoints are various transport encryptions. The MQTT broker supports the authentication between communicating devices utilizing MQTT protocol. TLS supports authentication and supports the usage of certificates for authorizing communication. The MQTT can approve or reject connections with clients depending on the client response to request for tokens. It is possible to further protect against unauthorized access through the combination of TLS (transport layer security) and a token-based authentication process (application layer security).

**DDoS/ Natural Disasters**

In the case where systems, servers, clients, cannot communicate due to disruption of service, the control for this risk is geo-redundancy, and backups.

**Physical Security**:

Unauthorized Access: If the wristband is not adequately secured to the wearer's wrist, it could be easily removed or stolen, potentially granting unauthorized access to sensitive data, or allowing someone else to use it fraudulently.

Tampering: The physical components of the wristband, such as the NFC tag or chip, could be tampered with, replaced, or modified, compromising the integrity of the wristband's functionality or data.

**Malicious Software**:

Malware and Viruses: If the wristband's software or firmware is vulnerable to malware or viruses, it could compromise the device's integrity, functionality, or the data it holds.

Firmware Exploits: Unpatched or outdated firmware may contain known vulnerabilities that could be exploited by attackers.

**Data Storage and Encryption**:

Inadequate Encryption: If the wristband stores sensitive data, such as patient information, inadequate or weak encryption methods could make it easier for attackers to access and exploit the data.

Data Leakage: Improper handling or storage of data on the wristband itself, or during data transfer, may lead to data leakage if appropriate security measures are not in place.

# NFC Communication Vulnerabilities

**Description**: Eavesdropping, data modification, and relay attacks can compromise the security

and integrity of NFC communication between the wristband and an NFC-enabled device.

**Detection**: Monitoring network traffic for unusual patterns, implementing tamper detection mechanisms, and conducting security assessments can help identify potential NFC communication vulnerabilities.

**Deterrence**: Implementing strong encryption algorithms, using secure protocols, and regularly updating NFC firmware can deter attackers from exploiting NFC communication vulnerabilities.

**Mitigation/Prevention**: Employing mutual authentication between the wristband and the NFC-enabled device, implementing secure coding practices, and integrating integrity checks can help mitigate NFC communication vulnerabilities.

**Physical Security**:

**Description**: Unauthorized access and tampering with the physical components of the wristband can compromise its integrity and the security of the data it holds.

**Detection**: Implementing tamper-evident seals, utilizing surveillance systems, and employing access logs can help detect physical security breaches.

**Deterrence**: Using secure wristband attachment mechanisms, implementing stringent access control measures, and raising awareness about the consequences of tampering can deter unauthorized physical access.

**Mitigation/Prevention**: Employing strong wristband attachment mechanisms, implementing anti-tamper measures, conducting regular physical security audits, and training staff on proper handling and reporting of suspicious activities can help mitigate physical security vulnerabilities.

**Malicious Software**:

**Description**: Malware and viruses can compromise the wristband's integrity, functionality, and the data it holds.

**Detection**: Utilizing antivirus software, conducting regular security scans, and monitoring for suspicious activities can help detect the presence of malicious software.

**Deterrence**: Ensuring all software and firmware updates are promptly applied, employing code signing and integrity checks, and educating users about the risks of installing unauthorized software can deter attackers from exploiting software vulnerabilities.

**Mitigation/Prevention**: Applying security patches and updates regularly, using reputable software sources, implementing secure boot mechanisms, and conducting periodic security assessments can help mitigate the risk of malicious software.

Other Potential Vulnerabilities

**Unauthorized access to an employee wristband**. This vulnerability refers to the possibility of unauthorized individuals gaining access to an employee’s wristband, potentially leading to data corruption. Detection could be challenging since it relies on identifying unauthorized physical access to the wristband. In order to deter this, Regular employee training and awareness programs can help deter unauthorized access attempts. For Mitigation and prevention, implementing MQTT security measures at the network, transport, and application layers can protect against unauthorized access and ensure secure communication between MQTT endpoints. This can include measures such as network layer protection with VPN or physically secured connections, as well as transport encryption to ensure data confidentiality.

**Weak data encryption leading to a data breach.** This vulnerability involves the use of weak data encryption algorithms, potentially leading to a data breach and compromising customer data. Some of the things that can help prevent this from occurring are regular security audits, vulnerability assessments, and penetration testing. Implementing strong encryption algorithms and regularly updating encryption protocols can deter potential attackers. Employing robust encryption algorithms and secure key management practices can mitigate the risk of a data breach. This includes using industry-standard encryption algorithms, ensuring secure key generation, storage, and rotation, and regularly updating encryption protocols to address emerging threats.

**Service disruption due to system failure.** This vulnerability refers to the potential disruption of services due to the system failures in the cloud infrastructure or IoT devices, impacting the availability and reliability of the product. System monitoring and logging can help detect system failures and irregularities real-time. Implementing redundant systems, such as fail-overs, and backup power supplies can minimize the likelihood of service disruptions. Ensuring regular maintenance of the cloud infrastructure and IoT devices, conducting periodic system health checks, and having redundant systems in place can mitigate the risk of service disruptions. Additionally, implementing backup and disaster recovery mechanisms can help minimize the impact of system failures.

**Unauthorized access to APIs.** This vulnerability involves unauthorized access to the APIs, potentially leading to data breaches or misuse of system functionalities. Monitoring API access logs and analyzing access patterns can help detect unauthorized access attempts. Implementing robust authentication and authorization mechanisms can deter unauthorized access to APIs. Implementing authentication mechanisms such as API keys, OAuth, or JWT tokens can control access to APIs. Additionally, implementing backup and disaster recovery mechanisms can help minimize the impact of system failures.

**Loss of data during transmission.** This vulnerability refers to the risk of data loss during transmission, potentially impacting patient data and analytics data. Implementing error detection and correction mechanisms can help detect data loss during transmission. Ensuring a reliable network infrastructure and minimizing environmental factors that could disrupt data transmission can deter data loss. Implementing data backup mechanisms, employing error detection and correction algorithms, and using reliable and secure transmission protocols can mitigate the risk of data loss during transmission. Regular monitoring and testing of data transmission can also help identify and address potential vulnerabilities.

# Appendix A

**Incidence Response Plan (IRP)**

## Incident Response Plan (IRP)

1. A person discovering the incident will notify a ground member/staff of the incident.

* Hospital Staff - notify in a timely manner so that they may efficiently take action according to protocol. Usually not specific contact information. Procedures would be to notify other staff of the incident and contact specified teams mentioned below.
* Visiting Medical Personnel - notify in a timely manner so that they may efficiently take action according to protocol. Usually have personal numbers/work phones where they can be contacted if need be. Procedures would be to notify other staff of the incident and contact specified teams mentioned below.
* Hospital Security Personnel - notify in a timely manner and would check cameras for more information in their investigation procedures. Usually not specific contact information, the room has a phone number to contact this department. Procedures would be to notify other staff of the incident and contact specified teams mentioned below.
* Law Enforcement - notified in a timely manner, in the event that apprehension of a suspect to further conduct investigation, they would be notified. Usually no personal contact information, the operator will route the call if need be. Procedures would be to notify other staff of the incident and conduct their investigation thoroughly.
* Senior Staff - notified in a timely manner if the situation becomes more entangled and difficult in nature. Usually specific contact information. Procedures would be to notify teams of the incident and contact specified team managers mentioned above to get a broader view of the situation.
* IT department/IR - notified in a timely manner to respond to incidents and check logs/checksums/event logs. Usually specific contact information. Procedures would be to notify teams of incidents, and organize aggregate log information, in combination with everything above to be able to see where to focus on.

1. If the person discovering the incident is a member of the Information Technology department, they would go on to step #5.
2. If the person discovering the incident is not a member of the Information Technology department, they would go on to contact the IT department at 321-444-4444 Ext 44. And contact appropriate teams like the Hospital Security Department at 321-444-4444 Ext 12.
3. The Hospital Security department will refer any and all technological emergencies to the IT emergency contact. Security department has been briefed to create their own log of the information including but not limited to:

* Incident discoverer
* Time of incident discovery
* Contact information of discoverer of incident
* Nature of incident
* What equipment or persons were involved?
* Location of equipment or persons involved.
* How the incident was detected

1. The IT staff member or affected department staff member who receives the call (or discovers the incident) will refer to their contact list for both management personnel to be contacted and incident response members to be contacted. The staff member will call those designated on the list. The staff member will contact the incident response manager using both email and phone messages while being sure other appropriate and backup personnel and designated managers are contacted. The staff member will log the information received in the same format as the ground’s security office in the previous step. The staff member could possibly add the following.

a) Is the equipment affected business critical?

b) What is the severity of the potential impact?

c) Name of system being targeted, along with operating system, IP address, and location.

d) IP address and any information about the origin of the attack.

1. Contacted members of the response team will meet or discuss the situation over the telephone and determine a response strategy.

a) Is the incident real or perceived?

b) Is the incident still in progress?

c) What data or property is threatened and how critical is it?

d) What is the impact on the business should the attack succeed? Minimal, serious, or critical?

e) What system or systems are targeted, where are they located physically and on the network?

f) Is the incident inside the trusted network?

g) Is the response urgent?

h) Can the incident be quickly contained?

i) Will the response alert the attacker and do we care?

j) What type of incident is this? Example: virus, worm, intrusion, abuse, damage.

1. An incident ticket will be created. The incident will be categorized into the highest applicable level of one of the following categories:

a) Category one - A threat to public safety or life.

b) Category two - A threat to sensitive data

c) Category three - A threat to computer systems

d) Category four - A disruption of services

1. Team members will establish and follow one of the following procedures basing their response on the incident assessment:

a) Worm response procedure

b) Virus response procedure

c) System failure procedure

d) Active intrusion response procedure - Is critical data at risk?

e) Inactive Intrusion response procedure

f) System abuse procedure

g) Property theft response procedure

h) Website denial of service response procedure

i) Database or file denial of service response procedure

j) Spyware response procedure.

1. Team members will use forensic techniques, including reviewing system logs, looking for gaps in logs, reviewing intrusion detection logs, and interviewing witnesses and the incident victim to determine how the incident was caused. Only authorized personnel should be performing interviews or examining evidence, and the authorized personnel may vary by situation and the organization.
2. Team members will recommend changes to prevent the occurrence from happening again or infecting other systems.
3. Upon management approval, the changes will be implemented.
4. Team members will restore the affected system(s) to the uninfected state. They may do any or more of the following:

a) Re-install the affected system(s) from scratch and restore data from backups if necessary. Preserve evidence before doing this.

b) Make users change passwords if passwords may have been sniffed.

c) Be sure the system has been hardened by turning off or uninstalling unused services.

d) Be sure the system is fully patched.

e) Be sure real time virus protection and intrusion detection is running.

f) Be sure the system is logging the correct events and to the proper level.

1. Documentation—the following shall be documented:

a) How the incident was discovered.

b) The category of the incident.

c) How the incident occurred, whether through email, firewall, etc.

d) Where the attack came from, such as IP addresses and other related information about the attacker.

e) What the response plan was.

f) What was done in response?

1. Evidence Preservation—make copies of logs, email, and other communication. Keep lists of witnesses. Keep evidence as long as necessary to complete prosecution and beyond in case of an appeal.
2. Notify proper external agencies—notify the police and other appropriate agencies if prosecution of the intruder is possible. List the agencies and contact numbers here.
3. Assess damage and cost—assess the damage to the organization and estimate both the damage cost and the cost of the containment efforts.
4. Review response and update policies—plan and take preventative steps so the intrusion can't happen again.

a) Consider whether an additional policy could have prevented the intrusion.

b) Consider whether a procedure or policy was not followed which allowed the intrusion, and then consider what could be changed to ensure that the procedure or policy is followed in the future.

c) Was the incident response appropriate? How could it be improved?

d) Was every appropriate party informed in a timely manner?

e) Were the incident-response procedures detailed and did they cover the entire situation? How can they be improved?

f) Have changes been made to prevent a re-infection? Have all systems been patched, systems locked down, passwords changed, antivirus updated, email policies set, etc.?

g) Have changes been made to prevent a new and similar infection?

h) Should any security policies be updated?

i) What lessons have been learned from this experience?

# Appendix B

**Privacy Impact Assessment (PIA)**

## Privacy Impact Assessment

Abstract

The abstract is the single paragraph that will be used to describe the program and the PIA. It will be published on the DHS web site and Federal Register. It should be a minimum of three sentences and a maximum of four, and conform to the following format:

• First sentence should include the name of the component and the system, technology, pilot, rule, program, or other collection (hereinafter referred to as “project”). Note: There are some instances where system is specifically called out.

• Second sentence should be a brief description of the project and its function.

• Third sentence should explain the reason the program is being created and why the PIA is required. This sentence should embody the same analysis that caused the project to be identified as a “privacy sensitive system” in the PTA, such as the project requires PII, or the technology is privacy sensitive.

The Hosp.ID.ality project is an innovative healthcare solution aimed at enhancing patient safety and improving operational efficiency in hospitals. By utilizing near-field communication (NFC) technology and real-time tracking, the project enables healthcare staff to monitor patient locations, streamline care delivery, and provide peace of mind to designated family members. This Privacy Impact Assessment (PIA) is conducted to ensure the privacy and security of personal information collected and processed within the system, recognizing the privacy sensitivity inherent in handling patient data and the need to comply with privacy regulations in healthcare environments.

**Overview**

The overview creates the foundation for the entire PIA. The overview provides the context and background necessary to understand the project’s purpose and mission and the justification for operating a privacy sensitive project. Include the following:

• Describe the purpose of the system, technology, pilot, rule, program, or other collection (hereinafter referred to as “project”) the name of the Department Component(s) who own(s) or is funding the project, the authorizing legislation, and how it relates to the components and Department’s mission.

• Describe how the project collects and uses PII, including a typical transaction that details the life cycle from collection to disposal of the PII; and

Describe the recommendation for how the program has taken steps to protect privacy and mitigate the risks described in the previous bullet. Note: Do not list every privacy risk in the succeeding analysis sections. Rather, provide a holistic view of the risks to privacy.

Additionally, consider the following as appropriate to the project:

Describe the funding mechanism (contract, inter-agency agreement) that the project will operate under:

Describe any routine information sharing conducted by the project both within DHS components and with external sharing partners and how such external sharing is compatible with the original collection of the information Analyze the major potential privacy risks identified in the analysis sections of the

PIA and discuss overall privacy impact of the program on individuals; and

Identify the technology used and provide a brief description of how it collects information for the project.

The Hosp.ID.ality project is a comprehensive healthcare solution developed to enhance patient safety, improve operational efficiency, and streamline care delivery in hospitals. The project is funded by a combination of investors, which include the Department of Health and Human Services (HHS), private healthcare organizations, and private research institutions. They all align their mission to promote the health and well-being of individuals. The project operates under the authority of relevant healthcare regulations, including HIPAA (Health Insurance Portability and Accountability Act) and other applicable privacy laws.

The Hosp.ID.ality project collects and utilizes personally identifiable information to facilitate real-time tracking and monitoring of patients within the hospital premise, also known as PII. PII collected may include patient identification data, such as names and unique identifiers, as well as location information associated with patient movements. The typical life cycle of PII involves collection at the point of registration or admission, ongoing tacking and updates as patients move within the hospital, and secure disposal or removal of PII once patients are discharged or their information is no longer required.

To protect privacy and mitigate risks, the Hosp.ID.ality project has implemented several safeguards. These include the use of secure communication protocols to transmit and store PII, encryption of sensitive data, access controls to limit unauthorized access to patient information, and regular monitoring of the system for security vulnerabilities. Strict data retention and disposal policies are also in place to ensure the proper handling of PII throughout its life cycle.

The project operates under the funding mechanism of a contract between the HSS, all the other investors and our development team. This ensures accountability and adherence to privacy and security requirements. Routine information sharing within DHS components and with external partners is conducted in compliance with applicable laws and regulations, and sharing practices are compatible with the original collection purpose of the information.

In the analysis sections of the PIA, major potential privacy risks have been identified and thoroughly assessed. The overall privacy impact of the Hosp.ID.ality project on individuals is considered moderate, as the collection and use of PII is necessary for achieving the project’s goals of patient safety and efficient care delivery. The technology used in the project primarily relied on Near-field communication (NFC) devices, such as wristbands and readers, to collect information related to patient location and identification. These devices ensure seamless and accurate tracking within the hospital premises while maintaining data security and privacy.

**Section 1.0 Authorities and Other Requirements**

**1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?**

List all statutory and regulatory authority for operating the project, including the authority to collect the information listed in question 2.1. Explain how the statutory and regulatory authority permits collection and use of the information. A simple citation without more information will not be sufficient for purposes of this document and will result in rejection of a Privacy Impact Assessment. You must explain how the statutory and regulatory authority permits the project and the collection of the subject information. If the project collects Social Security numbers, you must also identify the specific statutory authority allowing such collection.

If you are relying on another component and/or agency, please list their legal authorities.

Where information is received from a foreign government pursuant to an international agreement or memorandum of understanding, cite the agreement and where it can be found (i.e., website).

*Example: Section 4011 of the Intelligence Reform and Terrorism Prevention Act of 2004, 49 U.S.C. § 44903(h)(4) (2004).*

The National Conference of State Legislatures have 31 states with data disposal laws, since they are not all coinciding and uniform, we apply the NIST standard framework for IoT devices (SP 800-213) to better assist in staying compliant to most legal requirements on the federal, compliance, and state level.

**1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?**

For all collections of PII where the information is retrieved by a personal identifier, the Privacy Act requires that the agency publish a SORN in the *Federal Register*. Include the *Federal Register* citation for the SORN. If the information used in the project did not require a SORN, explain why not.

In some instances, an existing SORN (program specific, DHS-wide, or Government-wide) may apply to the project’s collection of information. In other instances, a new SORN may be required.

For the "Hosp.ID.ality" project, the collection of personally identifiable information (PII) falls under the purview of the Privacy Act. As such, a System of Records Notice (SORN) is required to be published in the Federal Register.

The applicable SORN for this project would be "Health and Human Services/Department-019, Patient Identification and Privacy Records." This SORN provides the necessary information regarding the collection, storage, and usage of PII within the healthcare context.

Additionally, in cases where the project's information collection aligns with an existing SORN, such as "Department of Health and Human Services-wide-001, General Files System," the relevant portions of that SORN would also apply to the project.

If the project's information collection does not require a separate SORN, it may be because the project operates within an existing system that already has a published SORN covering similar types of information. In such cases, the project would adhere to the existing SORN and would not require a separate publication.

It is important to note that the specific SORN citations provided above are hypothetical and should be replaced with the actual SORNs applicable to the "Hosp.ID.ality" project based on the relevant agency and department's policies and practices.

**1.3 Has a system security plan been completed for the information system(s) supporting the project?**

Provide the date that the Authority to Operate (ATO) was granted or the date it is expected to be awarded. An operational system must comply with DHS Management Directive 4300A. Note that all systems containing PII are categorized at a minimum as “moderate” under Federal Information Processing Standards Publication 199. If the project does not trigger the C&A requirement, state that along with an explanation.

For a new project provide anticipated date of C&A completion. If the project does not include technology, state that here.

For the "Hosp.ID.ality" project, a system security plan (SSP) has been completed for the information system(s) supporting the project. The SSP outlines the security controls and measures in place to protect the confidentiality, integrity, and availability of the system and the personally identifiable information (PII) it handles.

The project has undergone the Certification and Accreditation (C&A) process, as required by DHS Management Directive 4300A. The anticipated date of completion for the C&A process is [insert anticipated date]. Once the C&A process is successfully completed, the system will be granted an Authority to Operate (ATO), indicating that it meets the necessary security requirements to operate.

As the project involves the handling of PII, it is categorized as "moderate" under the Federal Information Processing Standards Publication 199, which sets the minimum-security categorization for systems containing PII.

**1.4 Does a records retention schedule approved by the National**

**Archives and Records Administration (NARA) exist?**

The project manager, in consultation with counsel and the component records management officer, must develop a records retention schedule for the records contained in the project that considers the minimum amount of time necessary to retain information while meeting the needs of the project. After the project manager and component records management officer finalize the schedule based on the needs of the project, it is proposed to NARA for official approval. Consult with your records management office for assistance with this question if necessary. If a NARA-approved schedule does not exist, explain what stage the project is in developing and submitting a records retention schedule.

Note: All projects may not require the creation of a new retention schedule.

The project manager, in consultation with counsel and the component records management officer, has developed a comprehensive records retention schedule for the records contained in the Hosp.ID.ality project. The schedule was carefully crafted to meet the specific needs of the project while ensuring compliance with applicable legal and regulatory requirements regarding record retention. For instance, records sent to records center storage in a NARA facility should have a remaining retention of at least 1 year, as stated in transmittal NO.22.

The team conducted a thorough analysis of the types of records generated by the project, considering their significance, sensitivity and the corresponding retention periods mandated by relevant laws and regulations. The retention schedule was designed to strike a balance between retaining records for an appropriate duration and minimizing unnecessary storage of information.

Following the development of the records retention schedule, it has been submitted to the National Archives and Records Administration (NARA) for official approval. This step ensures that the retention schedule aligns with federal regulations and establishes the necessary for retaining and disposing of the project’s records in a compliant manner.

The project is currently awaiting NARA’s review and approval of the proposed records retention schedule. This process reflects the project’s commitment to responsible records management and compliance with regulatory requirements to safeguard information throughout its lifecycle.

**1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.**

OMB Control Number(s):

0937-0198 Public Health Service Policies on Research Misconduct.

0915-0379 Questionnaire and Data Collection Testing, Evaluation, and Research for the Health Resources and Services Administration (HRSA)

**Section 2.0 Characterization of the Information**

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

**2.1 Identify the information the project collects, uses, disseminates, or maintains.**

Identify (1) the categories of individuals for whom information is collected, and (2) for each category, list all information, including PII, that is collected and stored by the project.

This could include, but is not limited to: name, date of birth, mailing address, telephone number, social security number, e-mail address, zip code, facsimile number, mother’s maiden name, medical record number, bank account number, health plan beneficiary number, any other account numbers, certificate/license number, vehicle identifier including license plate, marriage record, civil or criminal history information, medical records, device identifiers and serial numbers, education record, biometric identifiers, photographic facial image, or any other unique identifying number or characteristic.

If the project or system creates new information (for example, a score, analysis, or report) describe how this is done and the purpose of that information.

(1) The categories of individuals for whom information is collected include the following:

Patient, Health care provider, and emergency contact for the patient.

(2) The information collected will include patient biometrics, patient location data, patient name, telephone number, emergency contact information, medical record identifier, health insurance identifier.

If the project receives information from another system, such as a response to a background check, describe the system from which the information originates, including what information is returned and how it is used.

This project does not receive any additional information such as a background check. The information is queried into a database through a cloud API and the information stays local to those services. Any information returned from said databases is used only to display information like location, name, and room number of a patient.

**2.2 What are the sources of the information and how is the information collected for the project?**

A project may collect information directly from an individual, receive it via computer readable extract from another system, or create the information itself. List the individual(s) providing the specific information identified in 2.1.

If information is being collected from sources other than the individual, including other IT systems, systems of records, commercial data aggregators, and/or other Departments, state the source(s) and explain why information from sources other than the individual is required.

In some instances, DHS may collect information using different types of technologies such as radio frequency identification data (RFID) devices, video or photographic cameras, and biometric collection devices.

The information is sourced through initially through patients, medical id cards, or worst-case scenario, visitors who accompany the patient. This information is then entered into the RFID wristband, and used to query databases any time the patient is brought around or relocated from room to room.

**2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.**

Commercial data includes information from data aggregators such as Choice Point or Lexis Nexis, where the information was originally collected by a private organization for non-governmental purposes, such as marketing or credit reporting.

Publicly available data includes information obtained from the internet, news feeds, or from state or local public records, such as court records where the records are received directly from the state or local agency, rather than from a commercial data aggregator.

State whether the commercial or public source data is marked within the system.

*Example: The commercial data is used as a primary source of information regarding the individual. Alternatively, the commercial data is used to verify information already provided by or about the individual.*

There is no public data that is used for this project. All the information is generated on premise by the patients/visitors.

**2.4 Discuss how accuracy of the data is ensured.**

Explain how the project checks the accuracy of the information. Describe the process used for checking accuracy. If a commercial data aggregator is involved, describe the levels of accuracy required by the contract. Sometimes information is assumed to be accurate, or in R&D, inaccurate information may not have an impact on the individual or the project. If the project does not check for accuracy, please explain why.

Describe any technical solutions, policies, or procedures focused on improving data accuracy and integrity of the project.

*Example: The project may check the information provided by the individual against any other source of information (within or outside your organization) before the project uses the information to make decisions about an individual.*

To ensure accuracy of information, the project team will conduct research and development, and will conduct test runs prior to fully deploying the Hosp.id.ality product at a contracting party’s location (e.g., hospital). The documentation of the test run will check on the accuracy of data collection. Further procedures focused on improving data accuracy and integrity of project development include the participation and collaboration of internal party auditors, and external party auditors.

**2.5 Privacy Impact Analysis: Related to Characterization of the**

**Information**

Given the specific data elements collected, discuss the privacy risks identified and for each risk explain how it was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included.

Consider the following Fair Information Practice Principles (FIPPs) below to assist in providing a response:

*Principle of Purpose Specification:* Explain how the collection ties with the purpose of the underlying mission of the organization and its enabling authority.

*Principle of Minimization:* Is the information directly relevant and necessary to accomplish the specific purposes of the program?

*Principle of Individual Participation:* Does the program, to the extent possible and practical, collect information directly from the individual?

*Principle of Data Quality and Integrity:* Are there policies and procedures for DHS to ensure that personally identifiable information is accurate, complete, and current?

Follow the format below.

**Privacy Risk:** The risk of collecting excessive or irrelevant personally identifiable information (PII) that is not directly relevant or necessary for the purpose of the Hosp.ID.ality project.

**Mitigation:** The Hosp.ID.ality project adheres to the principle of minimization by collecting only the PII that is directly relevant and necessary to accomplish the specific purposes of the program. The data elements collected, such as patient room information and unique identifiers, are essential for real-time tracking, ensuring patient safety, and streamlining care delivery. The program avoids collecting excessive PII that is unrelated to its mission and purpose.

**Privacy Risk:** The risk of not providing individuals with the opportunity to participate or provide consent in the collection of their personal information.

**Mitigation:** The Hosp.ID.ality program incorporates the principle of individual participation by collecting information directly from the individuals themselves. This is achieved through the use of wristbands that are assigned to each patient, allowing them to have control and visibility over their own information. Individuals are informed about the purpose of the data collection and have the opportunity to consent to the use of their information for tracking and safety purposes.

**Privacy Risk:** The risk of inaccurate, incomplete, or outdated personally identifiable information being collected and stored.

**Mitigation:** The Hosp.ID.ality program has implemented policies and procedures to ensure data quality and integrity. Measures are in place to regularly update and maintain the accuracy, completeness, and currency of the collected PII. This includes periodic reviews and audits of the data, as well as data validation mechanisms to identify and correct any inaccuracies or discrepancies. Data integrity is crucial to ensure the effectiveness and reliability of the tracking system.

**Section 3.0 Uses of the Information**

The following questions require a clear description of the project’s use of information.

**3.1 Describe how and why the project uses the information.**

List each use (internal and external to the Department) of the information collected or maintained. Provide a detailed response that states how and why the different data elements will be used. If Social Security numbers are collected, state why the SSN is necessary and how it was used.

*Example: A project needs to collect name, date of birth, and passport information because that information provides the best matching capabilities against the terrorist screening database.*

The reason why the information like patient name, location, and is used is to provide the utmost of service to those coming in for medical attention. By using this information that is confidential, hospital staff will be able to find a patient, provide care for them, and much more in a timely manner. Reducing response time would only be beneficial to a patient in urgent care or any type of need.

**3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.**

Many projects sift through large amounts of information in response to user inquiry or programmed functions. Projects may help identify areas that were previously not identifiable and need additional research by agents, analysts, or other employees. Some projects perform complex analytical tasks resulting in other types of data, matching, relational analysis, scoring, reporting, or pattern analysis.

Discuss the results generated by the uses described in 3.1, including a background determination, link analysis, a score, or other analysis. These results may be generated electronically by the information system or manually through review by an analyst. Explain what will be done with the newly derived information.

Will the results be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.

*Example: The system will generate a response that there is a possible match to the terrorist screening database. This possible match will be maintained in the system with the information previously provided by the individual. A trained analyst will review the possible match and make a determination as to whether or not the individual is on the list. This determination will also be maintained in the system.*

The project does not necessarily use technology to conduct queries or analysis beyond well-made scripting to implement queries on Azure’s database software. To detect anomalies the use of good queries and query optimization in a timely manner would be the best way to implement these plans by the appropriate staff. Utilizing the data retention aforementioned, a record to a certain degree will be maintained in the event a user was to come back before data retention is over.

**3.3 Are their other components with assigned roles and responsibilities within the system?**

Discuss the intra-Departmental sharing of information (CBP to ICE). Identify and list the name(s) of any components or directorates within the Department with which the information is shared.

*Example: Certain systems regularly share information because of the crossover of the missions of the different parts of DHS. For example, USCIS employees regularly use a CBP system to verify whether an individual has entered the country. USCIS employees note that the CBP system has been checked and the date on which it was checked, but do not copy the information to the USCIS system.*

The project does not interact with other components unless the government has a federal need to access health information. For example, in such a case as transferring a patient to a local jail, or in such a case where law enforcement transfers the patient to other detention centers (Federal, State Prison) then the law enforcement agency will receive assigned roles and responsibilities within the system to permit access to patient data.

**3.4 Privacy Impact Analysis: Related to the Uses of Information**

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above.

*Example: Describe if training for users of the project covers how to appropriately use information. Describe the disciplinary programs or system controls (i.e., denial of access) that are in place if an individual is inappropriately using the information.*

Consider the following FIPPs below to assist in providing a response:

*Principle of Transparency:* Is the PIA and SORN, if applicable, clear about the uses of the information?

*Principle of Use Limitation*: Is the use of information contained in the system relevant to the mission of the project?

Follow the format below.

**Privacy Risk:** RFID skimming to grab information, unauthorized access to wristband with elevated privileges, MITM (man in the middle) attacks.

**Mitigation:** To reduce the potential of RFID skimming, the strict use of exclusive NFC technologies will mitigate all skimming attempts to more close range. Unauthorized access to a wristband will be mitigated by constant training of employees not to leave them laying around and always report if one is found. In the event they are taken off premise, there are signal deployers that zero out the wristband, so they do not have any elevated credentials stored once taken outside the premises.

**Section 4.0 Notice**

The following questions seek information about the project’s notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

**4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.**

In many cases, agencies provide written or oral notice before they collect information from individuals. That notice may include a posted privacy policy, a Privacy Act statement on forms, a PIA, or a SORN published in the *Federal Register*. Describe what notice was provided to the individuals whose information is collected by this project. If notice was provided in the *Federal Register* provide the citation, (e.g., XX FR XXXX, Date).

If notice was provided in a Privacy Act statement, attach a copy of the notice for review. Describe how the notice provided for the collection of information is adequate to inform those impacted.

Consult your privacy office and legal counsel on issues concerning the notice to the public for an information collection such as a form.

If notice was not provided, explain why. For certain law enforcement projects, notice may not be appropriate – this section of the PIA would then explain how providing direct notice to the individual at the time of collection would undermine the law enforcement mission.

The patient healthcare provider should inform the patient at first verbally, and also, should provide a pamphlet that provides the patient with full notice on the collection of information. The patient should provide an acknowledgement to their healthcare provider that they have understood and accepted the terms of the collection. Upon agreement between patient and health staff on patient acknowledgement, the medical staff will retain a copy of the patient’s acknowledgment to the Hosp.id.ality data collection and provide a copy to the patient of their acknowledgement.

**4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?**

This question is directed at whether the individual from or about whom information is collected can decline to provide the information and if so, whether the consequences of providing the information are included in the notice.

Additionally, state whether an individual may provide consent for specific uses or whether consent is given to cover all uses (current or potential) of his/her.

information. If specific consent is permitted or required, how does the individual consent to each use?

If notice is provided to explain how an individual may exercise the right to consent to particular uses or decline to provide information describe the process. If this is not an option, explain why not. In some cases, declining to provide information simply means the individual chooses not to participate in the project.

For patients to opt out of releasing their information they would be prompted to either accept or decline during the patient intake process. If they decide to opt out later on their information being displayed or used in a local database, they will have to wait until the appropriate IT personnel are able to drop it from the database.

**4.3 Privacy Impact Analysis: Related to Notice**

Discuss how the notice provided corresponds to the purpose of the project and the stated uses. Discuss how the notice given for the initial collection is consistent with the stated use(s) of the information. Describe how the project has mitigated the risks associated with potentially insufficient notice and opportunity to decline or consent.

Consider the following FIPPs below to assist in providing a response:

*Principle of Transparency*: Has sufficient notice been provided to the individual?

*Principle of Use Limitation:* Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?

*Principle of Individual Participation*: Has the program provided notice to the individual of how the program provides for redress including access and correction, including other purposes of notice such as types of information and controls over security, retention, disposal, etc.?

Follow the format below.

**Privacy Risk:** Insufficient notice and opportunity to decline or consent.

**Mitigation:**  TheHosp.ID.ality project recognizes the importance of providing clear and comprehensive notice to individuals regarding the purpose of the project and the stated uses of their personal information. To address this risk, the project has developed a robust entice framework that ensures transparency and enables individuals to make informed decisions.

The notice provided to individuals corresponds to the purpose of the project and the stated uses of the information. It clearly articulates the objectives of Hosp.ID.ality, including enhancing patient safety and improving hospital operations. The notice describes the types of information that will be collected, such as patient identification data and location information, and explains how this information will be used to facilitate efficient and secure patient management.

**Section 5.0 Data Retention by the project**

The following questions are intended to outline how long the project retains the information after the initial collection.

**5.1 Explain how long and for what reason the information is retained.**

The purpose of this question is to identify the specific types of information the project retains. Is all the information the project collects retained? Is there a specific subset of information retained?

*Example: A project may collect extensive PII initially for the purpose of verifying the identity of an individual for a background check. Upon completion of the background check, the project will maintain the new information, the results of the background check (approved/not approved) and delete all application information.*

This section should explain the nexus between the original purpose for the collection and this retention period. The minimum amount of information should be maintained for the minimum amount of time in order to support the project.

*Example: The project retains the information for the period of time in which fraud could be prosecuted and then the information is deleted.*

In some cases, DHS may choose to retain files in active status and archive them after a certain period of time. State active file retention periods as well as archived records, in number of years, as well as the approved or proposed NARA records schedule. Discuss when the time periods begin for inputs, outputs, and master files. Project managers should work with component records officers early in the development process to ensure that appropriate retention and destruction schedules are implemented.

The information collected does not require extended retention because minimal information is collected on the patient. The information collected does not add, or remove, from patient records, as it serves mostly to act as a tool of convenience. Patient location data will not need data retention past its duration of usage.

**5.2 Privacy Impact Analysis: Related to Retention**

Discuss the risks associated with the length of time data is retained. How were those risks mitigated?

Although establishing retention periods for records is a formal process,

there are policy considerations behind how long a project keeps information. The longer a project retains information, the longer it needs to secure the information and assure its accuracy and integrity. The proposed schedule should match the requirements of the Privacy Act to keep the minimum amount of PII for the minimum amount of time, while meeting the Federal Records Act. The schedule should align with the stated purpose and mission of the system.

Consider the following FIPPs below to assist in providing a response:

*Principle of Minimization:* Does the project retain only the information.

necessary for its purpose? Is the PII retained only for as long as necessary and relevant to fulfill the specified purposes?

*Principle of Data Quality and Integrity:* Has the PIA described policies and procedures for how PII that is no longer relevant and necessary is purged?

Follow the format below.

**Privacy Risk:** Data Leakage due to mismanaged older documents.

**Mitigation:** The mitigation to this privacy risk should incorporate restrictions to data retention. The master agreement document signed between the Hosp.id.ality team and the contracting party should include contract language to discuss the usage and purpose of limited data retention, and a document that prohibits over 2 years of data retention.

**Section 6.0 Information Sharing**

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state, and local government, and private sector entities.

**6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.**

Discuss the external Departmental sharing of information (for example, CBP to FBI). Identify the name or names of the federal agencies and foreign governments.

*Example: Customs and Border Protection may share biographic information on an individual with the Federal Bureau of Investigation in order for FBI to conduct a background check. Alternatively, USVISIT may share biographic and biometric information with the intelligence community in order to identify possible terrorists.*

For state or local government agencies, or private sector organizations list the general types rather than the specific names.

*Example: The program shares information with state fusion centers that have a posted privacy policy. In particular, discuss any international agreements that require information sharing as part of normal agency operations.*

6.1 Information Sharing:

As part of its normal agency operations, the Department may share information with various organizations to fulfill its mission. The specific organizations and methods of access may vary depending on the nature of the information and the purpose of sharing. Some examples of external sharing of information can include:

1. Federal Agencies: The Department may share information with other federal agencies such as the Federal Bureau of Investigation (FBI), Immigration and Customs Enforcement (ICE), or the Transportation Security Administration (TSA). Information may be accessed through secure data sharing platforms or established protocols to ensure proper handling and use.

2. State and Local Government Agencies: Information sharing with state and local government agencies may occur to support collaborative efforts in areas such as emergency management, law enforcement, or homeland security. Examples may include sharing information with state fusion centers or local law enforcement agencies. Access and usage of information would be governed by applicable laws, regulations, and privacy policies.

3. Private Sector Organizations: In certain cases, the Department may share information with private sector organizations, such as critical infrastructure operators or industry associations, to enhance situational awareness, cybersecurity, or national security efforts. Information sharing would typically occur through established channels and agreements, ensuring compliance with legal and privacy requirements.

4. International Agreements: Depending on international agreements or treaties, the Department may share information with foreign governments or international organizations as part of cooperative efforts in areas such as counterterrorism, border security, or intelligence sharing. These information sharing activities would be conducted in accordance with applicable laws, regulations, and bilateral or multilateral agreements.

It's important to note that the specific organizations and methods of information sharing will depend on the operational requirements and legal frameworks applicable to the Department's mission. The Department follows established policies and procedures to ensure appropriate access, use, and protection of shared information while adhering to privacy and security guidelines

**6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.**

Note which routine uses support the sharing described in 6.1 related to normal business operations.

*Example: Routine use H allows DHS to share biographic information with the FBI to conduct a background check. This is compatible with the original collection because the Immigration and Naturalization Act (INA) requires that USCIS determine whether an individual has committed any disqualifying crimes. Without checking with the FBI, DHS would be unable to meet this requirement of the law.*

The information provided in the Patient information segment of the SORN would fall under the Information Sharing SORN due to the fact that if there were officials in investigation with sufficient rights like a warrant, the information would have to be disclosed to them to a certain capacity. Both of these SORN’s go hand in hand for this very reason.

**6.3 Does the project place limitations on re-dissemination?**

Describe any limitations that may be placed on external agencies further sharing the information provided by DHS. In some instances, the external agency may have a duty to share the information, for example through the information sharing environment. But before disclosing the information to the individual the external agency is required to verify with DHS.

The possible limitation of an agency disseminating information that does not have the rights to this information would have to be verified through the DHS. Since we are only purveying the information to the authorities there would not be much in our jurisdiction beyond that fact. Possibly there could be a checksum implemented to make sure that the adequate personnel are viewing it only.

**6.4 Describe how the project maintains a record of any disclosures outside of the Department.**

Under subsection (c) of the Privacy Act, DHS must retain an accounting of what records were disclosed to whom, even for systems that are otherwise exempt from certain provisions of the Act. A project may keep a paper or electronic record of the date, nature, and purpose of each disclosure, and name and address of the individual or agency to whom the disclosure is made. If the project keeps a record, list what information is retained as part of the accounting requirement. A separate system does not need to be created to meet the accounting requirement, but the program must be able to recreate the information noted above to demonstrate compliance. If the project does not, explain why not.

The records that are maintained of any disclosure outside of the department is held for a year minimum electronically in an aggregate cloud software. Whatever agency that has received this disclosure will have to sign an agreement for adherence to federal and state regulations. The information that is retained would be the departments, individuals involved and a log of all emails/communications back and forth. All compiled into one log.

**6.5 Privacy Impact Analysis: Related to Information Sharing**

Discuss the privacy risks associated with the sharing of information outside of the Department. How were those risks mitigated?

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.

Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.

Follow the format below.

**Privacy Risk:** Data leakage due to external mismanagement of data

**Mitigation:** The contracting party and the Hosp.id.ality team should incorporate audit logs as a necessary procedure to reduce the risk of external data leakage, this language should become a part of the master agreement document signed between both parties.

**Section 7.0 Redress**

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

**7.1 What are the procedures that allow individuals to access their information?**

Describe any procedures or regulations your component has in place that allow access to information collected by the system or project and/or to an accounting of disclosures of that information. Generally speaking, these procedures should include the Department’s FOIA/Privacy Act practices. If the Privacy Act does not apply, state why this is the case. If additional mechanisms exist, include those in this section. For example, if your component has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the Department’s procedures.

If the system is exempt from the access provisions of the Privacy Act, explain the basis for the exemption and cite the Final Rule published in the Code of Federal Regulations (CFR) that explains this exemption. If the project is not a Privacy Act system, explain what procedures and/or regulations are in place that cover an individual gaining access to his/her own information.

Individuals would not have access to their information as it is only being used on a display and on a database accessed by personnel. If the user wanted to access their data, they would communicate with a staff member and they would be able to see their information and explained in real time. But as aforementioned, the concept of least privileges would be incorporated.

**7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?**

Discuss the procedures for individuals to address possibly inaccurate or erroneous information. If the correction procedures are the same as those given in question 7.1, state as much. If the system has exempted itself from the provisions of the Privacy Act, explain why individuals may not access their records.

Individuals, patients, will see their own information. The contracting agency will allow patients to submit tickets to correct erroneous information. The contracting agency will notify the Hosp.id.ality team of erroneous information reported from patients, and/or staff members.

**7.3 How does the project notify individuals about the procedures for correcting their information?**

Individuals may be made aware of redress procedures through the notices described above in Section 4 or through some other mechanism. This question is meant to address the risk that even if procedures exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are weakened significantly.

*Example: Some programs provide the information related to redress in a letter when an individual is given an initial negative determination regarding receiving a particular benefit. This would give the individual clear notice of how to address possible problems with the information the Department holds on him. Other programs depend upon a notice in the workplace rather than direct notice to the individual, so redress may be more difficult for the individual.*

The project will notify individuals of the procedures behind project data collection through notices, and emailed documentation to patient portal sites. The patient will receive an electronic and physical copy of full disclosure on data collection, and their health care provider will receive a copy of the patient’s acknowledgement of the received document.

**7.4 Privacy Impact Analysis: Related to Redress**

Discuss what, if any, redress program the project provides beyond the access and correction afforded under the Privacy Act and FOIA.

*Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.*

*Example: If a project does not allow individual access, the risk of inaccurate data needs to be discussed in light of the purpose of the project. For example, providing access to ongoing law enforcement activities could negatively impact the program’s effectiveness because the individuals involved might change their behavior.*

Consider the following FIPPs below to assist in providing a response:

*Principle of Individual Participation*: Is the individual provided with the ability to find out whether a project maintains a record relating to him?

*Principle of Individual Participation*: If access and/or correction is denied, then is the individual provided notice as to why the denial was made and how to challenge such a denial?

*Principle of Individual Participation*: Is there a mechanism by which an individual is able to prevent information about him obtained for one purpose from being used for other purposes without his knowledge?

Follow the format below.

**Privacy Risk:**

Privacy risk concerning things such as patient records. The Hosp.id.ality will keep a record of the user, for potential use in case the user wishes to one day access them. The individual will have the right to be informed that their data is being collected and used for future use. The individual will also have the right to access that information and receive a copy on how it's being used. However, the information may also be collected by other individuals based on situations such as an ongoing investigation. The user's data may be accessed by a private investigator to be used as evidence against the user if the user has committed a heinous crime.

**Mitigation:**

Mitigating the potential risk of user data being collected from unknown sources will be top priority. In such cases the user will be provided with a policy agreement that will state that their information will be collected for future use. However, the project team and management will help prevent any unauthorized access from anyone. The purpose of the user’s data being collected is to help improve security on IoT devices to help insure data protection across all devices. If the user wishes to request access to their information, but is prevented, they can look over at the policy agreement in which they signed before obtaining the device.

**Section 8.0 Auditing and Accountability**

The following questions are intended to describe technical and policy-based safeguards and security measures.

**8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?**

Auditing measures are recommended and should be discussed, but other possible technical and policy safeguards such as information sharing protocols, special access restrictions, and other controls should be discussed here as well.

Do the audit measures discussed above include the ability to identify specific records each user can access? Describe the different roles in general terms that have been created to provide access to the project information. For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.

Explain whether the project conducts self-audits, third party audits, reviews by the Office of Inspector General or Government Accountability Office (GAO).

Does the IT system have automated tools to indicate when information is possibly being misused?

*Example: If certain celebrity records are accessed, a supervisor is notified and reviews to ensure that the records were properly used.*

External auditors will visit contracted parties to audit their practices and adherence to PIA policies. Prior to completion of the project the Hosp.id.ality team will require the contracting party to sign a Master Agreement document which will include their agreement to holding their employees liable for data misuse, and their Identity Access Management (IAM) team, (internal or outsourced), will document authorized users listed with their permissions. This document will also require safe handling, as the users with higher permissions may become targeted if the permissions are revealed to external parties.

**8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.**

DHS offers privacy and security training. Each project may offer training specific to the project, which touches on information handling procedures and sensitivity of information. Discuss how individuals who have access to PII are trained to appropriately handle it.

Explain what controls are in place to ensure that users of the system have completed training relevant to the project.

In order to ensure users complete privacy training relevant to this project, the Hosp.id.ality project team will publish free privacy training, mandated through HR, published on corporate training websites, or connected HR training websites such as Workday. This medium should enable multiple corporations to validate user training through multiple avenues within the internal network. Granting full visibility to managers to check on employee privacy training status. However, training completion should become enforced from the user’s company’s HR. It should fall on the company to verify their own user training. The Hosp.id.ality project team will create relevant privacy training, and each business shall enforce user training on said training.

**8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?**

Describe the process and authorization by which an individual receives access to the information held by the project, both electronic and paper-based records. Identify users from other agencies who may have access to the project information and under what roles these individuals have such access. Describe the different roles in general terms that have been created that permit access to such project information.

Specifically, if remote access to the system is allowed or external storage or communication devices interact with the system, describe any measures in place to secure the transmission and storage of data (e.g., encryption and/or two- factor authentication).

*Example: Certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.*

The Hosp.id.ality team will set “least-privilege” access to most users thereby shielding user data from leakage as much as possible. Access to user data will require a need-to-know and will distribute minimal access to allow the user requesting access to conduct their job. The principle of least privilege is a pillar of zero trust network access framework 2.0. The implementation of least privilege depends upon cooperation between the Hosp.id.ality team and the contracting party. The contracting party shall develop a map of privileges and will send this map of privileges to the Hosp.id.ality team to implement user privileges based on the mapped configuration. For example, the contracting party maps network administrators as individuals that require higher access compared to hospital nursing interns. Upon completion of this map, the Hosp.id.ality team will configure user access in conjunction with the contracting party’s IAM team and will create a document (physical and electronic) that contains annually updated authorized users, and their permissions. External users with access to the project include “personal representatives” (health care providers), and individuals will have full access to their own health records collected from the project. The Hosp.id.ality project team will also ensure the contracting party signs a Master Agreement document prior to completion of services where the team will outline the need to enforce IAM (identity access management) information security oversight. The IAM oversight should also implement deprovisioning of temporary, or deleted accounts to avoid user data exposure. In addition to these measures, escalation of privilege will require several safeguards to prevent wrong user access. Re-evaluations of access will necessitate documentation and will necessitate approval from an employee’s immediate supervisor.

Data-in-transit, data-in-use, and data-at-rest will be encrypted. Remote access to the system will require monitoring from the contracting party’s SOC (security operations center) and connecting any unauthorized external storage devices to the Hosp.id.ality system (such as USB flash-drives) will require approval through the contracting party’s Enterprise Security Office GRC (governance, risk & compliance) team, in order to prevent data tampering.

**8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?**

The project shall review and approve information sharing agreements, MOUs, new uses of information, new access to the system by organizations with the company, through annual reviews conducted by program managers and through the employment of external auditors that shall verify the accuracy of information, and the mitigation of risks prescribed through healthcare security frameworks. Biennial reviews shall be conducted in conjunction with external auditors and internal auditors.