Data Security Overview

No direct data access is provided at any user level to the entire system. Access to functional sub-portals will be controlled at the user portal level by a sophisticated User Role Management (URM) module accessible only by administration staff. Each user group has customized screens presenting only data authorized for view by that group and allows review or editing based on access authorization.

QRyde Cloud is implemented on ITMS 7.0 platform and inherits all data safety protocols set up by HBSS' ITMS platform.

HIPAA Standards: Organizations covered under HIPAA have three choices: implement the specification as it appears in the Rule, implement an alternative that is equivalent to the specification, or document why the specification is not applicable and therefore is not implemented.

Organizations covered under HIPAA have three choices: implement the specification as it appears in the Rule, implement an alternative that is equivalent to the specification, or document why the specification is not applicable and therefore is not implemented. Data encryption and strong authentication are key components of the defense-in-depth principle. HBSS's applications use Transparent Data Encryption (TDE) to address Health Insurance Portability and Accountability Act (HIPAA) requirements.

Database Level Security Standards: The database system's RDBMS Advanced Security module supports the Advanced Encryption Standard (AES), DES, 3DES, and RC4 symmetric cryptosystems for protecting the confidentiality of RDBMS Net Services traffic.

The database system's RDBMS Advanced Security module supports the Advanced Encryption Standard (AES), DES, 3DES, and RC4 symmetric cryptosystems for protecting the confidentiality of RDBMS Net Services traffic. AES can be used by all U.S. government organizations and businesses to protect sensitive data over a network. This encryption algorithm defines three standard key lengths, which are 128-bit, 192-bit, and 256-bit. RDBMS Advanced Security provides the Data Encryption Standard (DES) algorithm. DES has been a U.S. Government standard for many years and is sometimes mandated in the financial services industry. Because it has been a standard for so long, DES is deployed throughout the world for use in a wide variety of applications.

Secure Email Notification: The system will be designed to send all outbound email using a server on a restricted network for the purpose of sending and receiving email. This server will support Transport Layer Security (TLS) which will encrypt outbound email in addition to decrypt inbound email.

Web Server Standards: The general standard is the use of HTTPS/SSL, which encrypts data transmitted via a website. ITMS's web server is an IIS (Internet Information Server). The IIS has the following security features: a) Basic Access Authentication, b) Digest Access Authentication, c) Integrated Windows Authentication, d) Client Certificate Mapping, e) IP Security, f) Request Filtering, and g) URL Authorization.

Inter-Application Communication: All transmission of data between applications, such as between ITMS and eligibility verification systems, will follow HIPAA protocols for electronic data interchange. All of ITMS's data extraction and uploads are fully secured.

Firewalls: HBSS has several firewalls which are configured to allow only specific protocols to connect to a De-Militarized Zone (DMZ); servers on a DMZ are allowed access to internal systems and outbound internet traffic. Servers on the DMZ are externally accessible and restricted to specific systems and ports.
Remote access communication: Remote access is restricted to only network users in HBSS's Active Directory. Network connections are established between the remote user and HBSS's firewall using a Virtual Private Network (VPN), which encrypts the connection.
Mobile Application Security: Enablement of Mobile Computing at the transportation level as well as encouraging the responder to propose solutions across the board. Specifically, functions such as route adherence: informing customers of ETA, providing real-time ridership data; and on consumer side: enabling members to schedule trips and file complaints.
This RFR requires enablement of Mobile Computing at the transportation level as well as encourages the responder to propose solutions across the board. Specifically, functions such as route adherence: informing customers of ETA, providing real-time ridership data; and on consumer side: enabling members to schedule trips and file complaints. The scope of mobile computing is vast, as it involves not only the mobile devices that the broker may provide to its inspectors, but also large number of independently owned devices running on different operating systems and platforms and that may have their own security and access controls. These devices will be multi-purpose, and the owners of the devices may simply not allow the standard Mobile Device Management (MDM) approaches such as enforcing a device password policy, device wipe outs, and lock outs. HBSS cannot provide devices to all vendor drivers or consumers, so HBSS is proposing a more sophisticated security paradigm – one that's primary objective is to secure brokerage data and prevent any data loss or theft. The mobile application device itself can be rendered useless by simply disabling password in case of reported device loss.
Mobile Data Terminals, Tablets, HBSS Phone Apps, and SMS Applications: HBSS will allow multiple types of devices that transportation providers may use to meet their requirements. HBSS will allow multiple types of devices that transportation providers may use to meet their requirements. These devices could be previously-installed Mobile Data Terminals and Automatic Vehicle Locators (MDT/AVLs). Providers using Tablets or SHBSS Phones and consumers using SHBSS Phones and SMS-enabled cell phones may be able to access information from ITMS (Integrated Transportation Management System).
ITMS Navigation Portal: HBSS will provide as part of ITMS a Navigation Portal which will enable vendor devices and consumer applications to connect to it and exchange data. Devices can connect either directly or indirectly via Secure Web Services Representational State Transfer Application Program Interface (RST-API).
HBSS will provide as part of ITMS a Navigation Portal which will enable vendor devices and consumer applications to connect to it and exchange data. Devices can connect either directly or indirectly via Secure Web Services Representational State Transfer Application Program Interface (RST-API). The applications will be a single unit (containerized) where the database and the application are one unit, so if there is a threat, the application self-destructs, wiping all data with it. When the application is not active, HBSS will require the applications to either have FIPS 140-2 Certified Cryptography or not have any data left on the device when in rest mode.

Mobile Security App Platform Options:HBSS will allow only those applications that are integrated with mobile security application platforms that meet HIPAA requirements. All high-security features must be monitored and controlled to ensure the communication channel remains secure.
Secure Back-End Server Connectivity: HBSS will support 2-tier architecture. Transportation providers who already have MDTs/AVL devices deployed may connect with ITMS Navigation Portal via SSL secure Web Services connectivity (REST API-Representational State Transfer Application Program Interface) protocol called NODE (New England Open Data Exchange), which is a transaction-based data exchange protocol.
HBSS will support 2-tier architecture. Transportation providers who already have MDTs/AVL devices deployed may connect with ITMS Navigation Portal via SSL secure Web Services connectivity (REST API-Representational State Transfer Application Program Interface) protocol called NODE (New England Open Data Exchange), which is a transaction-based data exchange protocol. A provider can develop proprietary applications and integrate them with ITMS via a back-end system, as well. Any back-end system involved in transferring data to ITMS will have to adhere to all security standards specified by HBSS.
Data Encryption: The application's security should be based on one or more of the following security protocols: a) Digital signature verification using 1024-bit to 4096-bit RSA; b) Hashing using the Secure Hash Algorithm (SHA-1); c) TDES encryption and decryption in ECB and CBC modes; d) AES encryption and decryption in ECB and CBC modes (NIST certificate #886); e) Secure random number generation (NIST certificate #508).
The application's security should be based on one or more of the following security protocols: a) Digital signature verification using 1024-bit to 4096-bit RSA; b) Hashing using the Secure Hash Algorithm (SHA-1); c) TDES encryption and decryption in ECB and CBC modes; d) AES encryption and decryption in ECB and CBC modes (NIST certificate #886); e) Secure random number generation (NIST certificate #508). The application will have to encrypt data using specified keys before transmitting and decrypt data when receiving. ITMS will have a receiver application that will accept all data connections and provide a secure web services library for applications to connect. Transportation Providers utilizing commercial applications must secure mobile applications and the data they use. Because device-level security isn't sufficient, especially with BYOD, security must be comprehensive, and it should be based on an end-to-end strategy that has accounted for the above requirements. By doing so, the Brokerage will have a comprehensive mobile application security experience that can keep sensitive data secure and prevent data loss.

QRyde Collocation Sites

HBSS is partnering with TierPoint services for the past 10 years, to host all of its virtualized environments in **Marlboro, MA** with **a backup at Andover, MA** facilities. We selected Tierpoint because we found it to be the right home for our mission critical QRyde Cloud.
As per TierPoint, their "data center facilities are designed to provide the highest levels of security, redundancy, and connectivity. Enterprise-class and carrier-neutral, their facilities feature unparalleled fiber connectivity and a physical infrastructure that delivers performance and protection."

As per TierPoint, Data Center components include:

- Redundant and diverse UPS systems
- Multiple on-site diesel generators
- Advanced fire detection and suppression
- Temperature-controlled environment
- Raised anti-static floors
- Physical security 24×7

TierPoint Power

TierPoint's power infrastructure provides the redundant, distributed, and diverse systems to keep all critical applications running around the clock. Their facilities use monitored power systems which include redundant generators, state-of-the-art paralleling gear with multiple distribution paths, on-site fuel capacity, and redundant and diverse UPS systems. Visit their power page for complete details.

TierPoint Cooling

State-of-the-art cooling systems keep data centers optimized for equipment to operate at peak. Each data center provides redundant data center cooling, humidity control systems, and multiple remotely monitored CRAC units.

TierPoint Safety & Protection

Advanced and early warning systems protect your investments. Their facilities are equipped with early warning smoke detection, gas, and dual pre-action dry pipe fire suppression systems as well as temperature and fire detection systems monitored 24/7.

TierPoint's multi-layered security systems keep IT assets safe and secure 24 hours a day, 7 days a week, 365 days a year. Each facility includes:

- On-site security staff
- Zoned physical security
- Closed-circuit surveillance
- Multiple dual-factored authentication zones
- Electronic key entry
- PIN access
- Biometric scan

QRyde Virtualized Environment

- Highly distributed processing engine (with multiple search/scheduling engines) processing multiple commands simultaneously and providing results simultaneously
- Virtual Infrastructure to support a database environment, and highly efficient map processing engine as well as multiple scheduling engines
- Provides high availability and fault tolerance
- Provides high degree of Data Protection both locally and off-site

It will optionally consist of

- SAN architecture for high speed data access

- Server-Class machines (linux or Windows) for setting up VMhost Cluster
- High speed redundant switch

All required Virtual Machines (VM) shall be created on top of this layer (VMhost). Host replication will ensure that any VM which goes down, restarts its replicated copy
The architecture supports different layers of security and HIPAA compliance as well as disaster recovery architecture.