

Phase 3 Data Privacy Plan (DPP)

Heart of Iowa Regional Transit Agency ITS4US Deployment Project

www.its.dot.gov/index.htm

Final Report — September 23, 2025
FHWA-JPO-22-971



U.S. Department of Transportation

Produced by Heart of Iowa Regional Transit Agency (HIRTA)
U.S. Department of Transportation
Intelligent Transportation Systems Joint Program Office
Federal Highway Administration
Office of the Assistant Secretary for Research and Technology
Federal Transit Administration

Notice

This document is disseminated under the sponsorship of the Department of Transportation in the interest of information exchange. The United States Government assumes no liability for its contents or use thereof.

The U.S. Government is not endorsing any manufacturers, products, or services cited herein and any trade name that may appear in the work has been included only because it is essential to the contents of the work.

Technical Report Documentation Page

1. Report No. FHWA-JPO-22-971		2. Government Accession No.		3. Recipient's Catalog No.	
4. Title and Subtitle Phase 3 Data Privacy Plan (DPP) – Heart of Iowa Regional Transit Agency ITS4US Deployment Project				5. Report Date November 4, 2025	
				6. Performing Organization Code	
7. Author(s) Josh Albertson; Santosh Mishra; Shauna Hallmark; Brooke Ramsey; Jenna Kubiak				8. Performing Organization Report No.	
9. Performing Organization Name and Address Heart of Iowa Regional Transit Agency (HIRTA) 2824 104 th St Urbandale, IA 50322				10. Work Unit No. (TRAIS)	
				11. Contract or Grant No. 693JJ32250012	
12. Sponsoring Agency Name and Address U.S. Department of Transportation ITS Joint Program Office 1200 New Jersey Avenue, SE Washington, DC 20590				13. Type of Report and Period Covered Final, Phase 3 (8/2024-2/2026)	
				14. Sponsoring Agency Code HOIT-1	
15. Supplementary Notes Elina Zlotchenko, Agreement Officer's Representative					
16. Abstract Heart of Iowa Regional Transit Agency (HIRTA) is one of four awardees of the ITS4US Phase 2/3. The deployment site for this project is Dallas County, located in central Iowa, west of Des Moines. This deployment will provide enhanced transportation access to healthcare options for all travelers in Dallas County. The project will deliver a solution to provide transportation access to healthcare facilities located in Dallas County using HIRTA and its contractor vehicles. The solution will enable coordination among HIRTA and its partners (e.g., Dallas County Health Department, healthcare providers, Medicaid providers, funding entities). The Data Privacy Plan (DPP) documents the data privacy approach and security controls of the Health Connector project team, including HIRTA, the MOD platform vendor, Flexlynqs/Varasi, NaviLens, and Iowa State University (ISU). The DPP includes strategies to mitigate the risk of harm to individuals that would result in the improper handling or disclosure of Personally Identifiable Information (PII) or Sensitive Personally Identifiable Information (SPII) collected from individuals in connection with the project.					
17. Keywords ITS4US, Healthcare, NEMT, MOD, PMP, ITS			18. Distribution Statement No restrictions		
19. Security Classif. (of this report) Unclassified		20. Security Classif. (of this page) Unclassified		21. No. of Pages 57	
				22. Price N/A	

Revision History

Name	Date	Version	Summary of Changes	Approver
Josh Albertson, IBI Group; Heidi Guenin, IBI Group	26 Sep 2022	0.1	Initial Draft	Brooke Ramsey
Josh Albertson, Arcadis IBI Group; Brianna Jasset, Arcadis IBI Group	13 October 2023	2.0	• New Table 1 on protections and permissions by user group • Revised public and private data tables • Revised document to reflect modifications made to PMESP • Updates from pre-MOD vendor selection	Brooke Ramsey
Josh Albertson, Arcadis IBI Group; Brianna Jasset, Arcadis IBI Group	9 February 2024	3.0	• Updated to address USDOT comments	Brooke Ramsey
Josh Albertson, Arcadis IBI Group; Brianna Jasset, Arcadis IBI Group	8 March 2024	4.0	• Updated to comply with 508 guidelines	Brooke Ramsey

Name	Date	Version	Summary of Changes	Approver
Josh Albertson, Flexlynqs Jenna Kubiak, Flexlynqs Santosh Mishra, Flexlynqs	7 March 2025	5.0	Updated Table 3 in section 2.2.1 in Phase 3 to reflect public data that could be collected. Aggregated summary no longer includes reference to funding program, deadhead miles, or statistics regarding underserved groups.	Brooke Ramsey

Name	Date	Version	Summary of Changes	Approver
Josh Albertson, Flexlynqs Jenna Kubiak, Flexlynqs Santosh Mishra, Flexlynqs	22 August 2025	6.0	- Updated throughout based on USDOT comments. This includes language, clarification on medical appointment data, and updated information about IRB approval. - Section 1: Updated to reflect additional changes made in DMP and in line with current USDOT guidelines. - Section 3.1: Updated to reflect Flexlynqs/Varasi as new Middleware vendor.	Brooke Ramsey
Josh Albertson, Flexlynqs Jenna Kubiak, Flexlynqs Santosh Mishra, Flexlynqs	23 September 2025	7.0	Updated based on USDOT comments - Section 2.5: Added clarification on public license - Updated revision history wording to clarify middleware vendor	

Revision History

Name	Date	Version	Summary of Changes	Approver
Josh Albertson, Flexlynqs Jenna Kubiak, Flexlynqs Santosh Mishra, Flexlynqs	4 November 2025	508	Updated to comply with 508 guidelines	Brooke Ramsey

This page intentionally left blank.

Table of Contents

Revision History	i
Table of Contents.....	vii
1 Introduction.....	1
1.1 Document Purpose	1
1.1.1 Organization of this Document	1
1.2 Deployment Concept.....	1
2 Privacy Approach.....	5
2.1 Access Requirements	5
2.2 Security Assessments.....	19
2.2.1 Public/Open Data.....	20
2.2.2 Private Data	22
2.2.3 Confidentiality, Integrity, and Availability (CIA) Assessment	32
2.3 Data Security Requirements	35
2.4 Risk Assessment of Threats	35
2.5 Data Sharing and Provision	37
2.6 Specific System Hardware Security Analysis.....	38
2.6.1 Traveler Personal Device	38
2.6.2 Transit Vehicle On-Board Equipment.....	38
2.6.3 HIRTA IT Hardware	38
2.6.4 Access2Care and Health Partner IT Hardware	39
2.6.5 Wayfinding Kiosks	39
3 Security Controls	41
3.1 Technical Controls.....	41
3.1.1 Cybersecurity.....	41
3.1.2 Data Security	42
3.1.3 Back-up and Recovery	43
3.2 Policy Controls.....	44
3.2.1 MOD vendor	44
3.2.2 NaviLens.....	45
3.2.3 Middleware vendor/Flexlynqs	45
3.2.4 ISU	45
3.3 Breach Plan.....	45
3.3.1 MOD vendor	45
3.3.2 NaviLens.....	45
3.3.3 Middleware vendor/Flexlynqs	45

3.3.4 ISU	46
Appendix A. Acronyms and Glossary.....	47
Appendix B. References	53
Appendix C. User Groups	55

List of Tables

Table 1. Protections and Permissions Applied to Each User Group	6
Table 2. Data Access Requirements	9
Table 3. Scope and Availability of Open/Public Data	21
Table 4. Scope and Availability of Private Data.....	23
Table 5. Confidentiality, Integrity, and Availability Assessment	33
Table 6. Dataset Risk Assessment.....	36
Table 7. Acronyms.....	47
Table 8. Glossary	49
Table 9. User Groups	55

List of Figures

Figure 1. Overview of Health Connector System Concept (Source: HIRTA Team)	2
Figure 2. Generic System Concept Diagram (Source: HIRTA team)	2

1 Introduction

1.1 Document Purpose

This Data Privacy Plan documents the privacy controls that will be applied to data collected, stored, and used throughout the implementation and evaluation of the Health Connector project. Data referenced in this document are discussed in greater detail in the Data Management Plan and comprise data identified in the ConOps [2], Human Use Approval Summary [6], and Performance Measurement and Evaluation Support Plan [3], with updates.

1.1.1 Organization of this Document

Section 1 of this DPP includes an overview of the DPP and of the Health Connector project. Section 2 describes the HIRTA team's privacy approach to and risk assessment of Health Connector data, presented by dataset and category, and including private and open data. Section 3 describes the controls that will be used to secure Health Connector data and respond to potential breaches.

1.2 Deployment Concept

The Heart of Iowa Regional Transit Agency (HIRTA) provides 300,000 customer rides and operates 95,000 hours (2019 estimates; pre-pandemic) along with 1.3 million miles of service within the seven-county region encircling the Des Moines urban area. HIRTA provides demand response services to customers for all trips booked from 24 hours to up to 14 days in advance. If capacity is available, HIRTA also provides trips to meet same day requests. HIRTA also acts as a service provider for the State of Iowa Medicaid broker, Access2Care.

HIRTA was awarded a Phase 2 agreement of the ITS4US contract for its proposed concept *"Health Connector: Bridging the Gap between Healthcare and Transportation"* (Health Connector) by the United States Department of Transportation (USDOT).

Health Connector is an innovative solution that will address various bottlenecks associated with transportation access to healthcare for HIRTA communities. Some of these challenges are key reasons behind missed appointments or the unacceptable level of preventive or as-needed healthcare in the HIRTA service area. For this deployment, the HIRTA team plans to implement a scalable and replicable solution that enables access to non-emergency medical transportation for all populations and their caregivers by resolving transportation access barriers with the use of advanced technologies. This solution will allow Dallas County residents without access to transportation who may be seeking a medical appointment to explore their transportation alternatives and book both medical and transportation appointments at the same time through a smart device (e.g., smartphone, smartwatch) application or equally effective alternate method. Further, this solution will include information and wayfinding services to guide them at every step of their trip.

[Figure 1](#) provides an overview of the Health Connector concept.

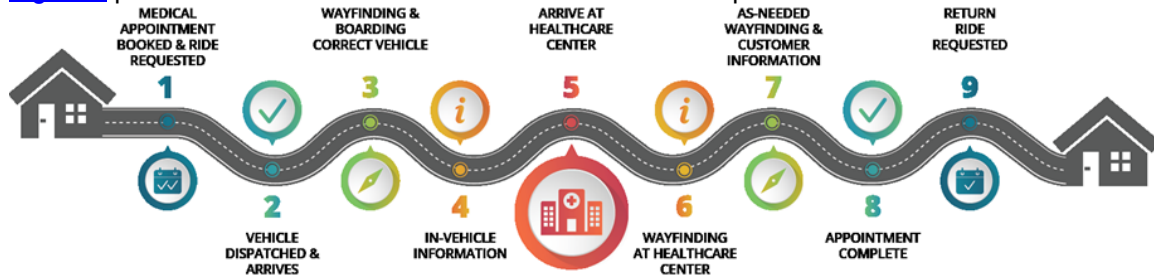


Figure 1. Overview of Health Connector System Concept (Source: HIRTA Team)

[Figure 2](#) provides a generic system context diagram with high-level flows.

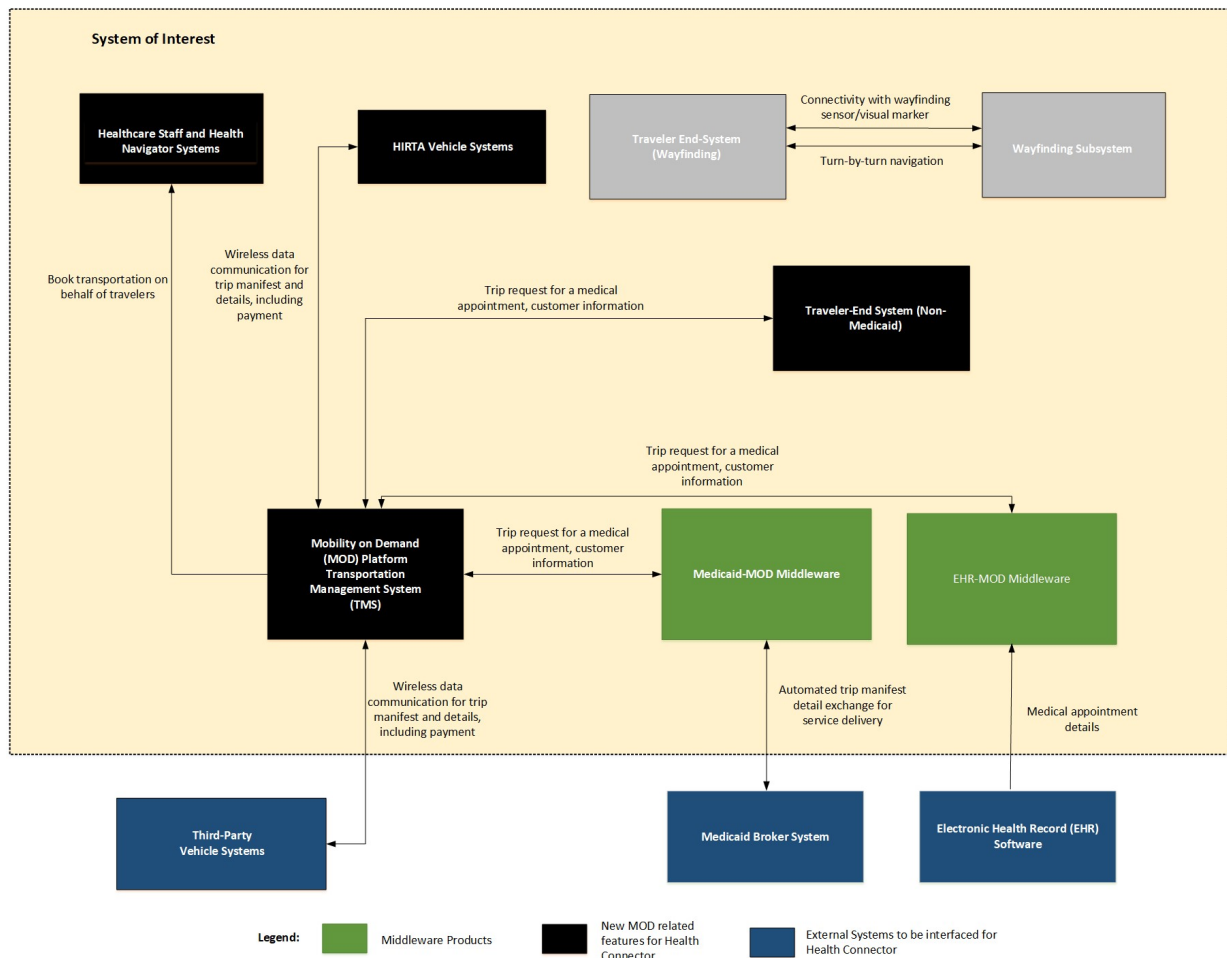


Figure 2. Generic System Concept Diagram (Source: HIRTA team)

U.S. Department of Transportation
Office of the Assistant Secretary for Research and Technology
Intelligent Transportation System Joint Program Office

There are five main goals for Health Connector, which include:

- Improved health outcomes through increased access to medical transportation for Dallas County residents
- Self-reliance and spontaneity for underserved groups
- Efficient transportation management capabilities for medical transportation services
- Financial sustainability of medical transportation programs
- Safe medical transportation services

For more information regarding these goals and more detailed objectives and performance measures, please see the Performance Measurement and Evaluation Support Plan (PMESP) [3]. Throughout, 'Traveler' refers to those individuals who will use Health Connector services to access healthcare appointments. Furthermore, vendors for the following systems have been determined and are identified below:

- MOD TMS Platform (Traveler app, Driver app, and Via Operations Center (VOC) – Via
- Wayfinding System – NaviLens
- Medicaid Broker System – Access2Care was identified as the Medicaid Broker System at the start of Phase 2. Access2Care was since acquired by MTM who will become the new Medicaid Broker for the state of Iowa

Throughout this document, generic terminology to describe these systems has been employed as to opposed to the selected vendor's platform to facilitate replication of a similar system by interested agencies.

2 Privacy Approach

2.1 Access Requirements

Data privacy is critical to protect Travelers that take part in Health Connector. As a first line of protection, Health Connector will only collect information critical to successful trips; sensitive information that is not required for trips (e.g., prescription history, Social Security numbers, etc.) will not need to be generated in the first place. As an additional layer of privacy protection, the HIRTA team has set access requirements for who is allowed to access specific types of data. Vendors associated with this project will not have the ability to ingest Health Connector data for their usage. Table 1 provides an overview of the protections and permissions applied to each user group. Table 2 provides an overview of the data access between system components and identifies which groups are eligible to send and receive data as part of the Health Connector system of interest (SOI). For information about sharing data related to the performance evaluation of Health Connector, please see the Data Management Plan. Please see [Appendix C](#) for descriptions of the user groups referenced in Table 1 and Table 2.

HIRTA will be the owner of all data generated by the system (exceptions listed in section [2.5 Data Sharing and Provision](#)), and most of the data generated by the Health Connector system will be collected, stored, processed, analyzed, and archived within the HIRTA TMS (for the provision of service and for relevant reporting and invoicing) and within the local ISU data system for performance evaluation, provision of controlled access for researchers and the Independent Evaluation team, and for public data provision for USDOT and the general public. Data collected and generated by the wayfinding system will be stored within that system and will be made available on-demand per HIRTA-defined terms and conditions.

For external systems from the Medicaid Broker and third-party service providers, data exchange will be based on open APIs, and relevant data will be stored within the HIRTA TMS per approved terms and conditions between HIRTA and external parties, as discussed in section [2.5 Data Sharing and Provision](#).

Table 2 identifies datasets in the context of existing and future systems at HIRTA. generic terminology to describe these systems has been used to facilitate replication of a similar system by interested agencies. The terminology used is common in paratransit/demand response industry and are applicable to most commercially available platforms/solutions This document extends information available in Table 2 of the DMP as it identifies the groups that will have the ability to send and access specific data.

Table 1. Protections and Permissions Applied to Each User Group

User Group	Abbreviation	Applied Protections and Permissions
Administration	ADM	Data is accessible only to those who have access to MOD platform TMS (VOC). Permissions are configurable by HIRTA and protected by unique login and 2-factor authentication.
Customer Service Staff	CSR	Data is accessible only to those who have access to MOD platform TMS (VOC). Permissions are configurable by HIRTA and protected by unique login and 2-factor authentication.
Third Party Service Provider	CTR	Data is accessible only once a third-party provider has been approved by HIRTA and has their shift added into the MOD Platform TMS. Drivers only receive first name and last initial along with mobility needs.
Driver	DRV	Data is accessible only once a third-party provider has been approved by HIRTA and has their shift added into the MOD Platform TMS. Drivers only receive first name and last initial along with mobility needs.
Funding Entity	FND	Funding entities receive data from HIRTA at the end of a month to reconcile trips and funds that were used. No PII is delivered when this data is transmitted, and access is limited to those within a given funding organization.
Healthcare Customer Care Staff	HCR	Access is limited based on permissions prescribed by HIRTA; health care providers and navigators may only see trip details for Travelers they are assisting and are protected from other functionality such as scheduling and dispatch. Login is also protected by 2-factor authentication.
Health Navigators	HNV	Access is limited based on permissions prescribed by HIRTA; health care providers and navigators may only see trip details for Travelers they are assisting and are protected from other functionality such as scheduling and dispatch. Login is also protected by 2-factor authentication.

User Group	Abbreviation	Applied Protections and Permissions
Independent Evaluator Team	IE Team	Access is governed by agreements between the HIRTA team and the IE team or other researchers. In such an event that data is shared under such an agreement, similar protections will be in place regarding file sharing password protections.
Iowa State University	ISU	ISU only accesses data that has been anonymized and aggregated and is stored in CyBox, a secure file storage system that is protected by FTPS.
MOD System	MOD	Data is accessible only to those who have access to MOD platform TMS (VOC). Permissions are configurable by HIRTA and protected by unique login and 2-factor authentication.
Transportation Operations Staff	OPS	Data is accessible only to those who have access to MOD platform TMS (VOC). Permissions are configurable by HIRTA and protected by unique login and 2-factor authentication.
Public	Public	No limitations on access are placed on this data
Researchers	Researchers	Access is governed by agreements between the HIRTA team and the IE team or other researchers. In such an event that data is shared under such an agreement, similar protections will be in place regarding file sharing password protections.
Traveler	TRV	Data being communicated to travelers such as trip status and vehicle location information is only communicated via configurable notifications and visible through the Traveler application. The traveler application is protected by 2-factor authentication login. Notifications protections are dependent on hardware security design such as phone or computer passcode.
USDOT	USDOT	Access is governed by the agreement between the HIRTA team and USDOT. Any data shared to USDOT through the ITS DataHub is considered a public dataset.

User Group	Abbreviation	Applied Protections and Permissions
Wayfinding System	WAY	Access to the wayfinding application is open to the public. Access to code configuration backend software is password protected and limited to identified individuals managing the system.

Table 2. Data Access Requirements

ID	Data	High-level Description	Systems Involved	Group(s) Sending Data	Group(s) Accessing Data
1	Traveler profile	Traveler's personal details as provided as part of registration. These details may be entered by the Traveler or by HIRTA CSRs. The Traveler profile may be accessed by the MOD platform and third-party transportation providers in the course of providing service but cannot be accessed or used for any purposes outside of required reporting, invoicing, and providing transportation services to the Traveler.	MOD platform	TRV, CSR	MOD, CTR, ADM, DRV, ISU
2	Traveler eligibility	Traveler's eligibility for a funding source or programs. These details may be entered by the Traveler or by HIRTA CSRs, will be verified with funding entities (e.g., Medicaid). Traveler eligibility may be accessed by the MOD platform and third-party transportation providers in the course of providing service but cannot be accessed or used for any purposes outside of required reporting, invoicing, and providing transportation services to the Traveler.	MOD platform, Eligibility management system/funding source	TRV, CSR, FND	MOD, CTR, ADM, ISU
3	Fleet information	Details on HIRTA's vehicles; also, details on third-party vehicles. These will be entered by HIRTA operations staff and third-party transportation providers. Fleet information will be used by the MOD platform and HIRTA administration and accessed by Travelers through the MOD platform.	MOD platform; third-party platform	OPS, CTR	TRV, MOD, ADM, ISU
4	Driver information	Details on HIRTA's drivers; also, details on third-party vehicles. These will be entered by HIRTA operations staff, HIRTA drivers, and third-party transportation providers. Driver information will be used by the MOD platform and HIRTA administration and accessed by Travelers through the MOD platform. This information can only be accessed and used for required reporting and for the provision of service to Travelers and cannot be accessed for other purposes.	MOD platform; third-party platform	DRV, OPS, CTR	TRV, MOD, ADM

ID	Data	High-level Description	Systems Involved	Group(s) Sending Data	Group(s) Accessing Data
5	Trip request	Traveler request for a trip from a web or mobile device. These details may be entered by the Traveler, HIRTA CSRs, health navigators, or healthcare customer care staff. Trip request information will be used by the MOD platform and accessed by HIRTA operations staff and third-party transportation service providers through the MOD platform in the course of providing service or fulfilling reporting requirements. Details also may be provided by Travelers via the middleware that connects with the Medicaid Broker-generated trip requests. Trip request information cannot be accessed or used for any purposes outside of required reporting, invoicing, and providing transportation services to the Traveler.	MOD platform	TRV, CSR, HNV, HCR	OPS, MOD, CTR, ADM, ISU
6	Trip cancellation	Traveler's request to cancel an existing trip. These details may be entered by the Traveler, HIRTA CSRs, health navigators, or healthcare customer care staff. Trip cancellation information will be used by HIRTA administration and the MOD platform and accessed by HIRTA drivers, HIRTA operations staff, and third-party transportation services providers through the MOD platform in the course of providing service or fulfilling reporting requirements. Details also may be provided by Travelers via the middleware that connects with Access2Care-generated trip requests. Trip cancellation information cannot be accessed or used for any purposes outside of required reporting, invoicing, and providing transportation services to the Traveler.	MOD platform, Health Connector middleware	TRV, CSR, HNV, HCR	DRV, OPS, ADM, MOD, CTR, ISU

ID	Data	High-level Description	Systems Involved	Group(s) Sending Data	Group(s) Accessing Data
7	Trip status	Current information on upcoming trip made available through the MOD platform, including automated information from third-party transportation service providers. Travelers may request status updates directly via the MOD platform or through HIRTA CSRs, health navigators, or healthcare customer case staff. Trip status information cannot be accessed or used for any purposes outside of providing transportation services to the Traveler.	MOD platform	CTR, MOD	TRV, CSR, HCR, HNV
8	Manifest	Time and location details on Travelers to be picked up and dropped off by a driver during a shift. This information will be generated through the MOD platform with input from HIRTA operations staff and will be accessed by HIRTA drivers. The manifest cannot be accessed or used for any purposes outside of required reporting, invoicing, and providing transportation services to the Traveler.	MOD platform	MOD, OPS	DRV, CTR, ADM
9	Vehicle location	Location and heading along with other details for a vehicle in service made available through the MOD platform. Travelers may request status updates directly via the MOD platform or through HIRTA CSRs. Vehicle location cannot be accessed or used for any purposes outside of providing transportation services to the Traveler.	MOD platform	MOD	TRV, CSR
10	Trip performance	Trip-level log of actual time and location for trips on the manifest along with any no-shows and cancellation events made available through the MOD platform, including information entered by HIRTA drivers. Information will be used by HIRTA administration and by CSRs when cancellation or no-show events impact the Traveler profile. Trip performance information cannot be accessed or used for any purposes outside of required reporting, invoicing, evaluating Health Connector performance, and providing transportation services to the Traveler.	MOD platform	DRV, MOD	CSR, ADM, ISU

ID	Data	High-level Description	Systems Involved	Group(s) Sending Data	Group(s) Accessing Data
11	Driver performance	Driver-level log of operational performance on log on, on-time performance, manifests completed made available through the MOD platform, including information entered by HIRTA drivers. Information will be used by HIRTA administration. Driver performance information cannot be accessed or used for any purposes outside of required reporting and providing transportation services to the Traveler.	MOD platform	DRV, CTR, MOD	ADM, ISU
12	Travel time	Time needed to perform on-board component of a trip made available through the MOD platform, including information entered by HIRTA drivers. Information will be used by HIRTA administration and by the ISU team for performance evaluation. Travel time information cannot be accessed or used for any purposes outside of evaluating Health Connector performance and providing transportation services to the Traveler.	MOD platform	DRV, CTR, MOD	ADM, ISU
13	Driver messages	Messages sent by drivers to dispatchers made available through the MOD platform. Information will be used by HIRTA operations staff and by ISU and HIRTA admin staff to provide insight into events that impact performance. Driver messages cannot be accessed or used for any purposes outside of evaluating Health Connector performance and providing transportation services to the Traveler.	MOD platform	DRV	OPS, ADM
14	Dispatcher messages	Messages sent by dispatchers to drivers made available through the MOD platform. Information will be used by HIRTA operations staff and by ISU and HIRTA admin staff to provide insight into events that impact performance. Dispatcher messages cannot be accessed or used for any purposes outside of evaluating Health Connector performance and providing transportation services to the Traveler.	MOD platform	OPS	DRV, ADM

ID	Data	High-level Description	Systems Involved	Group(s) Sending Data	Group(s) Accessing Data
15	Fare payment log	Log of amount paid for a trip and method of payment that will be entered directly by Travelers or drivers into the MOD platform. This information will be accessed directly by HIRTA administration and used for invoicing external organizations that fund trips. Fare payment information cannot be accessed or used for any purposes outside of required reporting, invoicing, and providing transportation services to the Traveler.	MOD platform	TRV, DRV	ADM, FND, ISU
16	Request for third-party trips	Time and location details on Travelers to be picked up and dropped off by a third-party driver during a shift. This information will be made available through the MOD platform and will be accessed by third-party drivers and by HIRTA administration for performance evaluation. The manifest cannot be accessed or used for any purposes outside of required reporting, invoicing, and providing transportation services to the Traveler.	MOD platform	MOD	CTR, ADM
17	Trip performance (third party)	Third-party provider trip-level log of actual time and location for trips on the manifest along with any no-shows and cancellation events made available through the MOD platform. Information will be used by HIRTA administration and by CSRs when cancellation or no-show events impact the Traveler profile. Trip performance information cannot be accessed or used for any purposes outside of required reporting, invoicing, evaluating Health Connector performance, and providing transportation services to the Traveler.	Third-party platform	CTR, MOD	ADM, CSR, ISU
18	Vehicle location (third party)	Location, heading of, and other details of a third-party provider vehicle in service, made available through the MOD platform. Travelers may request status updates directly via the MOD platform or through HIRTA CSRs. Vehicle location cannot be accessed or used for any purposes outside of providing transportation services to the Traveler.	Third-party platform	CTR	TRV, CSR

ID	Data	High-level Description	Systems Involved	Group(s) Sending Data	Group(s) Accessing Data
19	Driver messages (third party)	Messages sent by drivers to dispatchers, made available through the MOD platform. Information will be used by HIRTA operations staff or third-party dispatchers (depending on system configuration) and by ISU and HIRTA admin staff to provide insight into events that impact performance. Driver messages cannot be accessed or used for any purposes outside of evaluating Health Connector performance and providing transportation services to the Traveler.	MOD platform	CTR	OPS
20	Dispatcher messages (third party)	Messages sent by dispatchers to drivers made available through the MOD platform. Information will be used by HIRTA operations staff or third-party dispatchers (depending on system configuration) and by ISU and HIRTA admin staff to provide insight into events that impact performance. Dispatcher messages cannot be accessed or used for any purposes outside of evaluating Health Connector performance and providing transportation services to the Traveler.	MOD platform	CTR	OPS
21	Fare payment log (third party)	Log of amount paid for a trip and method of payment that will be entered directly by Travelers or third-party drivers into the MOD platform. This information will be accessed directly by HIRTA administration and used for invoicing external organizations that fund trips. Fare payment information cannot be accessed or used for any purposes outside of required reporting, invoicing, and providing transportation services to the Traveler.	Third-party platform	TRV, CTR	ADM, FND, ISU

ID	Data	High-level Description	Systems Involved	Group(s) Sending Data	Group(s) Accessing Data
22	Medicaid trip requests	Traveler request for Medicaid-funded trips from a web or mobile device through the Medicaid Broker; some Travelers may request over phone and use concierge service. Information will be transferred to the MOD platform via the Health Connector middleware, used by the MOD platform, and accessed by HIRTA operations staff and third-party transportation services providers through the MOD platform in the course of providing transportation services, invoicing, or fulfilling reporting requirements. Medicaid trip request information cannot be accessed or used for any purposes outside of those listed.	Medicaid broker system	TRV, FND	MOD, OPS, CTR, ISU
23	Medicaid trip performance	Trip-level log of actual time and location for trips on the manifest along with any no-shows and cancellation events for trips delivered for Medicaid-funded trips. Information will be made available through the MOD platform. Information will be used by HIRTA administration and by CSRs when cancellation or no-show events impact the Traveler profile. Medicaid trip performance information cannot be accessed or used for any purposes outside of required reporting, invoicing, evaluating Health Connector performance, and providing transportation services to the Traveler.	MOD platform	DRV, CTR,	ADM, CSR, ISU
24	Medical appointment details	Consists of medical appointment date, time, and location (facility address and doctor's office) for a particular Traveler. Data will be provided by Traveler or by healthcare customer care staff and will be used by MOD platform to allow for identification of appointment changes and accompanying transportation needs. Medical appointment details cannot be accessed or used for any purposes outside of providing transportation services to the Traveler.	EHR	HCR, TRV	MOD

ID	Data	High-level Description	Systems Involved	Group(s) Sending Data	Group(s) Accessing Data
25	Aggregated summary	Aggregated data on driver, vehicle, and trip performance, automatically generated by the MOD platform and used by HIRTA administration and ISU for performance evaluation.	MOD platform	MOD	ADM, ISU
26	Traveler wayfinding request	Requests initiated by Travelers to the wayfinding system. Traveler wayfinding requests cannot be accessed or used for any purposes outside of providing wayfinding services to the Traveler.	Wayfinding subsystem	TRV	WAY
27	Traveler wayfinding guidance	Log of wayfinding information provided to Travelers. Traveler wayfinding guidance cannot be accessed or used for any purposes outside of providing wayfinding services to the Traveler.	Wayfinding subsystem	WAY	TRV
28	Safety event	Log of incidents and accidents by vehicle/driver/trip.	MOD platform	DRV, OPS	ADM, ISU
29	Safety event report	Detailed reports by a safety event (incident, accident) with response.	HIRTA supporting systems	DRV, OPS	ADM, ISU
31	System performance	Email notifications of system wide failures and or downtime.	MOD platform; HIRTA supporting systems	MOD	ADM, ISU
32	Anonymized and/or aggregated data for performance evaluation	Anonymized/aggregated Traveler, trip, and operations data to support Health Connector performance evaluation. Data will be automatically generated by the MOD platform and created through other HIRTA systems and will be provided to ISU.	MOD platform	MOD, ADM	ISU
33	Traveler complaints log	Log of Traveler complaints received and actions taken. Information will be provided by the Traveler, drivers, or HIRTA CSRs and will be used by HIRTA operations and administration.	MOD platform; HIRTA supporting systems	TRV, DRV, CSR, CTR	OPS, ADM, ISU
34	Traveler survey results	Traveler data and survey conducted by ISU of human use participants. Information will be provided by Travelers directly and through Health Connector and will be used by ISU for performance evaluation. Final results will be shared back with Travelers.	MOD platform; local data system at ISU	TRV	ISU

ID	Data	High-level Description	Systems Involved	Group(s) Sending Data	Group(s) Accessing Data
35	Processed data for controlled sharing	Data based on Data ID #32 and #34, processed, hosted, and made available by ISU. Data will be accessible to researchers, independent evaluation team, and USDOT	CyBox	ISU	IE Team, Researchers
36	Public data for USDOT – managed system	Trip summary data and performance measurement results aggregated by time period will be provided. Other aggregated data such as fleet, vehicle, and safety event (incident/accident) information will also be provided. Data sharing will align format established through the ITS Datahub.	ISU Public Dashboard	ISU	USDOT, Public
37	Cost and revenue summary	Cost and revenue data by trip, including actual cost, fare paid, funding source share, automatically generated by the MOD platform or created through other HIRTA systems based on MOD platform and other data.	MOD platform; HIRTA supporting systems	MOD, ADM	ISU, ADM
38	Wheelchair failure log	Summary of events referring to situations when wheelchair lift could not function at the time of pick-up or drop-off. Wheelchair failure log data will be made available to ISU for the provision of data for public access (Data ID #36).	MOD platform; HIRTA supporting systems	DRV, OPS	ISU, ADM
39	Medical appointment status	Real-time status of progress on a medical appointment resulting in an impact on the pick-up time. Data will be provided by healthcare customer care staff and made available to the Traveler and driver through the MOD platform via the Health Connector middleware.	EHR	HCR	MOD, TRV, DRV, CTR
40	Discount coupon/credit	Discount coupons or credits applied by trip. Aggregated and/or anonymized Discount coupon/credit data may be accessed by ISU for evaluating Health Connector performance.	Eligibility management system/funding source	TRV, FND	MOD,FND, ISU

ID	Data	High-level Description	Systems Involved	Group(s) Sending Data	Group(s) Accessing Data
41	Call center log	Call center statistics available from HIRTA, DCHD and healthcare providers, as available from phone systems or manual logs. Log of Traveler complaints received and actions taken. Information will be used by HIRTA operations and administration.	HIRTA supporting systems	ADM, HCR, HOP	ADM, OPS, ISU
43	Trip request (partners)	Trips manually requested by DCHD and healthcare providers using HIRTA TMS. To be tracked separately to assess the benefit of such capability. Trip request information cannot be accessed or used for any purposes outside of required reporting, invoicing, evaluating Health Connector performance, and providing transportation services to the Traveler.	MOD platform	HNV, HCR, CHP	ADM, ISU

2.2 Security Assessments

To ensure data security and availability for the duration of Phase 2 and Phase 3 of the Health Connector project as well as for the five years that HIRTA has agreed to continue to provide Health Connector service after Phase 3, HIRTA will contract with ISU to continue to ensure relevant data is available for seven years. After Phase 3, the data that Health Connector will continue to generate and make available to the USDOT and to researchers through controlled access will be those data included as described in the following sections. Access level is defined for accessing data as follows:

- **Open** - Data that can be used by the public with no or limited licensing restrictions. This data is available to the public without needing to request permissions and will be provided to the USDOT-managed public system. These datasets will not contain any PII.
- **Private** - Data that cannot be shared with the public without being summarized (see data ID 27 for more information). Access to this data is limited and only granted with Institutional Review Board (IRB) and project team approvals. Private data will be available under the following subcategories of access levels:
 - **Vendor-collected data:** Data that the vendor collects through the app. These data are controlled through privacy and use agreements that participants agree to when they install the app. The HIRTA team has confirmed that the vendor's user agreement language aligns with the project needs and establishes sufficient informed consent. Data such as location, address, etc. will be collected to allow the app to provide information such as trip planning, etc. Unless extracted for project purposes, these data are not stored or utilized by the Health Connector team (including HIRTA's MOD vendor) for other purposes.
 - **Personal Identifiable Information (PII):** Data which is extracted from the app for project purposes or collected through other means such as user surveys and has PII included. The access to these data will be restrictive to protect the PII based on IRB-approved processes. Data in this category will have an operational purpose that justifies its storage. For Health Connector, it will include Traveler details (name, ID, location), driver details (name, ID, vehicle details), trip details (trip ID that can be linked to any personal identity), and medical appointment details (location and start/end time only) in the raw dataset, as well as any other dataset marked as PII as part of the IRB process. Any PII data from the app necessary for project purposes will be anonymized and aggregated as needed prior to storage within the ISU CyBox system and managed under their IRB. PII data collected during user surveys or other means will be collected, stored, and managed at ISU under their IRB.
 - **Proprietary:** Licensed data from third parties or data that can reveal details on proprietary methods and applications protected as part of intellectual property. This data will be used for operational purposes. Any access to the data is determined by usage agreements between the parties. Examples include pathways structure for wayfinding, or access to raw real-time data on service management from MOD vendor.

- **Research:** Data that is available under controlled access for independent research if an agreement is in place between the HIRTA team and researchers. Users of the data may need to meet IRB requirements before gaining access to the data. These datasets will still be anonymized and will not contain PII. Examples of this data include survey data, trip-level data, driver-level data, and Traveler-level data.

2.2.1 Public/Open Data

Data will be made available to the public in CSV format through the USDOT-managed ITS DataHub, and through a web-based dashboard hosted by ISU. ISU will process data from Traveler surveys (data ID #34) and anonymized and/or aggregated data for performance evaluation (data ID #32) to provide processed data for public sharing (data ID #36). Table 3 represents a detailed view of data ID #36, and information regarding relevant access portals and safeguarding methods that will be in place.

Data are categorized by datasets, defined as follows:

- **Admin:** includes data that is required for administrative needs prior to a trip being provided (e.g., customer registration, eligibility management, fleet management/maintenance). It also refers to any data that is part of routine process (e.g., safety management, complaints).
- **Driver:** includes driver-level details including name, vehicle used, and their service performance (revenue miles, revenue hour, on-time performance).
- **Trip:** includes trip-level data for Travelers and drivers including location, time, and fare payment. Traveler, driver, and trip identifiers are anonymized.
- **Aggregated:** refers to aggregated summary for a chosen time interval. Summary available at Traveler, driver /vehicle, provider, and trip level.
- **Survey:** refers to survey data and results. Details regarding this will be provided after the IRB process is complete.
- **Healthcare appointment:** refers to medical appointment related data, and any data collected by DCHD for health navigation purposes (external to System of Interest). HIRTA team does not plan to collect any other health-related data.
- **System log:** refers to data logged in the system to assess system performance and reliability. Also may include supportive information (e.g., communication log indicating traffic delay).
- **Wayfinding:** refers to log of requests and pathways directions provided at device level.

Table 3. Scope and Availability of Open/Public Data

ID	Data	Dataset	Access Portal	Safeguarding Methods and Processes
3	Fleet information	Admin	USDOT-managed system, ISU Dashboard	Active HIRTA fleet data will be made publicly available “as is” given it does not contain any PII or sensitive information. Active fleet data for contractors or TNCs will be made available excluding any PII (e.g., license plate), pending third-party contract provisions. The key purpose of making this dataset available will be to analyze capacity, reliability, and availability by vehicle.
25	Aggregated Summary	Aggregated	USDOT-managed system, ISU Dashboard	Aggregated trip summary data can be provided to give details on project performance without revealing granular data that may contain PII. Aggregated operational summary (trips completed, vehicles in use, average travel time, fare collected) by hour and provider will be provided, when aggregation provides sufficient privacy protection.
28	Safety event	Admin	USDOT-managed system, ISU Dashboard	Details involving HIRTA assets will be made available to report on safety events on a monthly basis. No PII will be included.
29	Safety event report	Admin	USDOT-managed system, ISU Dashboard	Details involving HIRTA assets will be made available to report on safety events along with any safety response taken on a monthly basis. No PII will be included.
38	Wheelchair failure log	Aggregated	USDOT-managed system, ISU Dashboard	Daily report on data aggregated at vehicle level will be available on wheelchair failure logs indicating number of failure events by vehicle.

2.2.2 Private Data

Controlled access to private data will be made available in CSV and/or JSON format to researchers and USDOT independent evaluators upon request. ISU will only have access to anonymized and/or aggregated data and will retain the data for the full 7 years of the project. The MOD vendor will be required, through their contract with HIRTA, to also maintain the raw data for the full 7 years of the project. ISU will process data from Traveler surveys (data ID #34) and anonymized and/or aggregated data for performance evaluation (data ID #32); these data IDs, in combination with other data IDs that cannot be shared for a variety of reasons described below, combine to represent processed data for controlled sharing (data ID #35), which is represented in Table 4. Data will be anonymized and aggregated within the MOD Platform TMS prior to transfer to CyBox and access by ISU. This data may then be linked by ISU to other datasets on underserved populations, through unique identifiers will be maintained to protect privacy. The aggregation and anonymization process is especially important for datasets that contain personally identifiable information (PII) and sensitive personally identifiable information (SPII). For the Health Connector project, data collected and exchanged with the MOD vendor about healthcare appointments may be considered SPII, as it may relate to the location of healthcare facilities that treat specific illnesses.

Table 4 represents the data, access portal, and safeguarding methods the Health Connector team will use. These data are categorized according to the same datasets as those listed in section [2.2.1 Public/Open Data](#).

Table 4. Scope and Availability of Private Data

ID	Data	Dataset	Access Portal	Reason(s) the Data is Private	Safeguarding Methods and Processes
1	Traveler profile	Admin	ISU CyBox	Research: This data consists of Traveler PII.	Aggregated and/or anonymized Traveler profile data collected by ISU for evaluating Health Connector performance will be made available. Aggregation and anonymization methods will occur within the MOD platform. Data can be aggregated by time period, service type, or geographic zone as needed. Unique Identifiers are used in place of names to help make data anonymous. <u>Included Data:</u> Anonymized traveler ID, mobility need, eligibility for funding sources (multiple sources may be applicable), recurring or ad-hoc trip customer.
2	Customer eligibility for a funding source	Admin	ISU CyBox	Research: This data consists of Traveler PII.	Approach taken for Data ID #1 provides the eligibility information.
4	Driver information	Driver	MOD platform	This information is not relevant to identified Health Connector performance measures and can only be accessed and used for required reporting and for the provision of service to Travelers and cannot be accessed for other purposes.	Not made available externally.

ID	Data	Dataset	Access Portal	Reason(s) the Data is Private	Safeguarding Methods and Processes
5	Trip request	Trip	MOD Platform, ISU CyBox, Middleware read-only web page	Research: Trip-level details include location and time information which can be used to reidentify a Traveler so is treated like PII.	Aggregated and/or anonymized Trip request data collected by ISU for evaluating Health Connector performance will be made available. Aggregation and anonymization will occur within the MOD platform; an anonymized, unique identifier for each trip with will be applied to origins and destinations. <u>Included Data:</u> Trip ID (anonymized), requesting device ID (anonymized), device type, pick-up location (aggregated), drop-off location (aggregated), pick-up time, drop-off time, whether or not request completed, gap in requested time and scheduled time, number of alternatives offered, amount of advanced notice in trip request.
6	Trip Cancellation	Trip	MOD Platform, ISU CyBox, Middleware read-only web page	Research: Trip-level details include location and time information which can be used to reidentify a Traveler so is treated like PII.	Same approach as Data ID #5 will be used. <u>Included Data:</u> Trip ID (anonymized), device id (anonymized), device type, original/modified pick-up location, original/modified drop-off location, original/modified pick-up time, original/modified drop-off time, whether or not request completed, gap in requested time and scheduled time.

ID	Data	Dataset	Access Portal	Reason(s) the Data is Private	Safeguarding Methods and Processes
7	Trip status	Trip	MOD Platform, Middleware read-only web page	Research: Trip-level details include location and time information which can be an issue if somehow Traveler identity is determined (e.g., looking up address in public records). Trip-level data will be made available only for research with an agreement that Traveler identity will be fully protected. Proprietary: Access to real-time data cannot be provided as continuous stream of real-time data can be used to reverse engineer proprietary algorithms. Trip status information cannot be accessed or used for any purposes outside of providing transportation services to the Traveler.	Not made available externally.
8	Manifest	Admin	Not available	Private dataset used for only internal operational purposes. Contains PII data. The manifest cannot be accessed or used for any purposes outside of required reporting, invoicing, and providing transportation services to the Traveler.	Not made available externally.
9	Vehicle location	Trip	Not available	This information is not relevant to identified Health Connector performance measures and can only be accessed and used for required reporting and for the provision of service to Travelers and cannot be accessed for other purposes.	Not made available externally.

ID	Data	Dataset	Access Portal	Reason(s) the Data is Private	Safeguarding Methods and Processes
10	Trip performance	Trip	MOD Platform, ISU CyBox, Middleware read-only web page	Research: Trip-level details include location and time information which can be used to reidentify a Traveler so is treated like PII. Proprietary: Access to real-time data cannot be provided as continuous stream of real-time data can be used to reverse engineer proprietary algorithms.	Same approach as Data ID #5 will be used. <u>Included Data:</u> Trip ID (anonymized), driver ID, vehicle ID, scheduled/actual pick-up location, scheduled/actual drop-off location, scheduled/ETA/actual pick-up time, scheduled/ETA/actual drop-off time, whether or not a no-show, no-show reason, whether or not cancelled, cancellation reason.
11	Driver performance	Driver	MOD Platform, ISU CyBox	Research: Raw driver-level data includes PII (name).	Aggregated and/or anonymized Driver performance data collected by ISU for evaluating Health Connector performance will be made available. <u>Included Data:</u> Driver ID, revenue miles, revenue hours, trips completed, revenue collected, rating
12	Travel time	Aggregated	MOD Platform, ISU CyBox	Proprietary: Access to real-time data cannot be provided, as continuous stream of real-time data can be used to reverse engineer proprietary algorithms.	Approach taken for Data ID #10 provides the Travel time information.
13	Driver messages	System log	Not available	This information is not made available through the MOD platform and is used for internal communications only.	Not made available externally.
14	Dispatcher messages	System log	Not available	Sensitive operational information which is not made available outside of operational context.	Not made available externally.

ID	Data	Dataset	Access Portal	Reason(s) the Data is Private	Safeguarding Methods and Processes
15	Fare payment log	Trip	MOD Platform, ISU CyBox	Research: Fare payment data is connected with trip performance data and contains PII.	Trip anonymization approach as discussed for Data ID #5 will be used to provide log of fare payment. <u>Included Data:</u> Trip ID, actual cost, fare required, fare paid, discount coupon/code, payment method.
16	Request for third-party trips	Admin	MOD Platform, ISU CyBox	Research: Trip-level details include location and time information which can be used to reidentify a Traveler so is treated like PII.	Same as Data ID #5. <u>Included Data:</u> Trip ID (anonymized), pick-up location, drop-off location, pick-up time, drop-off time, mobility aid requested, funding source requested, whether or not request completed, gap in requested time and scheduled time.
17	Trip performance (third party)	Trip	MOD Platform, ISU CyBox	Research: Trip-level details include location and time information which can be used to reidentify a Traveler so is treated like PII. Proprietary: Access to real-time data cannot be provided as continuous stream of real-time data can be used to reverse engineer proprietary algorithms.	Same approach as Data ID #5 will be used. <u>Included Data:</u> Trip ID (anonymized), vehicle ID, driver ID, scheduled/actual pick-up location, scheduled/actual drop-off location, scheduled/actual pick-up time, scheduled/actual drop-off time, whether or not a no-show, no-show reason, whether or not cancelled, cancellation reason.
18	Vehicle location (third party)	Trip	MOD Platform	This information is not relevant to identified Health Connector performance measures and can only be accessed and used for required reporting and for the provision of service to Travelers and cannot be accessed for other purposes.	Not made available externally.

ID	Data	Dataset	Access Portal	Reason(s) the Data is Private	Safeguarding Methods and Processes
19	Driver messages (third party)	System log	MOD Platform, ISU CyBox	This information is not made available through the MOD platform and is used for internal communications only.	Not made available externally.
20	Dispatcher messages (third party)	System log	MOD Platform, ISU CyBox	This information is not made available through the MOD platform and is used for internal communications only.	Not made available externally.
21	Fare payment log (third party)	Trip	MOD Platform	Research: Fare payment data is connected with trip performance data and contains PII. This information is not relevant to identified Health Connector performance measures.	Not made available externally.
22	Medicaid trips requests	Trip	MOD Platform, ISU CyBox, Middleware read-only web page	Research: Trip-level details include location and time information which can be used to reidentify a Traveler so is treated like PII.	Same approach as Data ID #5 will be used. <u>Included Data:</u> Trip ID (anonymized), pick-up location, drop-off location, pick-up time, drop-off time, whether or not request completed, gap in requested time and scheduled time.

ID	Data	Dataset	Access Portal	Reason(s) the Data is Private	Safeguarding Methods and Processes
23	Medicaid trip performance	Trip	MOD Platform, ISU CyBox, Middleware read-only web page	Research: Trip-level details include location and time information which can be used to reidentify a Traveler so is treated like PII. Proprietary: access to real-time data cannot be provided as continuous stream of real-time data can be used to reverse engineer proprietary algorithms.	Same approach as Data ID #5 will be used. <u>Included Data:</u> Trip ID (anonymized), scheduled/actual pick-up location, scheduled/actual drop-off location, scheduled/actual pick-up time, scheduled/actual drop-off time, whether or not a no-show, no-show reason, whether or not cancelled, cancellation reason.
24	Medical appointment details	Health	Middleware read-only web page	SPII: HIPAA-protected details.	Information is only accessible by approved users with access to middleware read-only webpages. Only includes information on appointment location and time. No specific health related data is being collected or transferred.
26	Traveler wayfinding request	Wayfinding	Not available	Proprietary: the format in which request is received is proprietary given there is no standard available. Research: Trip-level details include location and time information which can be used to reidentify a Traveler so is treated like PII.	Not made externally available.
27	Traveler wayfinding guidance	Wayfinding	Not available	Proprietary: the format in which direction is provided is proprietary given there is no standard available. Research: Trip-level details include location and time information which can be used to reidentify a Traveler so is treated like PII.	Not made externally available.

ID	Data	Dataset	Access Portal	Reason(s) the Data is Private	Safeguarding Methods and Processes
31	System performance	System log	Not available	Proprietary: details may include server logs that may reveal unintended information.	Not made externally available.
32	Anonymized and/or aggregated data for performance evaluation	Aggregated	ISU CyBox	Research: Data will be anonymized and/or aggregated before being shared with ISU. ISU will process the data further as needed to ensure cleanliness and privacy protection before making data available through Data ID #35 and ID #36, as relevant.	Same approach as Data ID #5 will be used. Planned data to be included: All data elements in Table 2 that include ISU as a 'Group Accessing Data.'
33	Traveler complaints log	Admin	MOD Platform, ISU CyBox	PII: may include some PII information.	Will be aggregated by complaint type and provider type at daily level for tracking customer complaints received. <u>Included Data:</u> customer complaint received, provider, date received, complaint date, resolution, and resolution date.
34	Traveler survey results	Survey	MOD Platform, ISU CyBox	PII: some PII information may be present. Research: will be made accessible for research, particularly to supplement findings from other analyses. Survey results will be critical for several performance measures.	HIRTA received IRB to collect data on and survey Health Connector riders. A survey has been deployed using Survey Monkey directly through the Health Connector application. In April 2025, HIRTA received updated IRB approval to perform data collection on existing HIRTA riders that are eligible for Health Connector. Additional consent from these riders was determined to be unnecessary due to lack of new data fields being collected.

ID	Data	Dataset	Access Portal	Reason(s) the Data is Private	Safeguarding Methods and Processes
37	Cost and revenue summary	Aggregated	ISU CyBox	Research: cost and revenue data are sensitive until finalized.	Data will be made available for research only. There are several factors involved in managing cost and revenue data, and sometimes it is not done until a reporting period is complete. As such, data based on formal request will be provided after proper validation. <u>Included Data:</u> Reporting period (monthly, quarterly, annual), number of trips completed, total revenue miles, total revenue hours, total cost, total revenue, total fare paid, total discount coupon/credits used, trips completed, number of Travelers served.
39	Medical appointment status	Middleware	Middleware read-only web page	SPII: HIPAA-protected details	Only limited information available indicating whether or not transportation access was provided for a medical appointment and if the medical appointment was a no-show. No specific health related data will be included. <u>Included Data:</u> Trip ID (anonymized), no-show status, no-show reason, dependent on ability of EHR and practice of healthcare facility to capture status and reason.
40	Discount coupon/credit	Trip	Not available	Same as Data ID #15 and #21	Not made available externally. Relevant information captured in Data ID #15 and #21.
41	Call center log	Admin	ISU CyBox	Same as Data ID #33	Same as Data ID #33.
43	Trip request (partners)	Trip	ISU CyBox	Same as Data ID #5	Same as Data ID #5.

2.2.3 Confidentiality, Integrity, and Availability (CIA) Assessment

Table 5 reflects 'low,' 'moderate,' and 'high' as defined in the ITS reference architecture and shared below [5].¹

- “The potential impact is LOW if the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to participants.
- The potential impact is MODERATE if the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or participants. A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.
- The potential impact is HIGH if the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. AMPLIFICATION: A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to participants involving loss of life or serious life threatening injuries.”

¹ With 'individuals' changed to 'participants' for the purposes of the Health Connector Project

Table 5. Confidentiality, Integrity, and Availability Assessment

Dataset	Confidentiality	Integrity	Availability
Admin - includes data that is required for administrative needs prior to a trip being provided (e.g., customer registration, eligibility management, fleet management/ maintenance). It also refers to any data that is part of routine process (e.g., safety management, complaints).	Moderate	Moderate	High
Driver - includes driver-level details including name, vehicle used, and their service performance (revenue miles, revenue hour, on-time performance).	Moderate	Moderate	High
Trip - includes trip-level data for Travelers and drivers including location, time, and fare payment. Traveler, driver, and trip identifiers are anonymized.	Moderate	Moderate	High
Aggregated - refers to aggregated summary for a chosen time interval. Summary available at Traveler, driver /vehicle, provider, and trip level.	Low	Low	Low
Survey - refers to survey data and results. Details regarding this will be provided after the IRB process is complete.	Low	Low	Low
Healthcare appointment - refers to medical appointment related data and any data collected by DCHD for health navigation purposes. This does not include health data and is limited to appointment location/time.	Moderate	Moderate	Moderate
System log - refers to data logged in the system to assess system performance and reliability. Also may include supportive information (e.g., communication log indicating traffic delay).	Low	Moderate	Moderate
Wayfinding - refers to log of requests and pathways directions provided at device level.	Moderate	Low	Low

General assessment related to data and system confidentiality, availability, integrity, and authenticity are provided below:

- **Confidentiality:** HIRTA will be the owner of all datasets for the data collected within HIRTA TMS (including data from the MOD TMS). Only authorized users, per their role,

are provided access to specific modules of the system and the data generated by those systems, as identified in the system configurations. For Health Connector, the data flow diagram by user group included in the ConOps will be used to identify access levels for system end users.

When medical appointment data is made available by the healthcare provider, an information release form will have to be signed by the parties accessing such information. Consent form is approved by both healthcare provider and patient/Traveler. No specific health related data will be collected or transferred.

Data within Access2Care and wayfinding systems will be made available to HIRTA per agreement signed by HIRTA with them, but currently both of those organizations are marked as the owners of data generated in their systems. Security that governs the API is covered through an NDA. Therefore, there will not be any public dissemination of the data from either organization.

- **Integrity:** System functions will be made available to HIRTA staff and its partners according to their roles and responsibilities. Except for those privileges, no user is authorized to make any changes. Also, system audit trail shows if and what changes were made by a user.
 - **Authenticity and non-repudiation:** Data sent and received between devices are logged with contextual information (e.g., vehicle to TMS messages have vehicle ID, location, and time stamp attached). Also, when trip requests are sent by customers, those will include the customer information, as only registered customers are allowed to book trips with HIRTA.
- **Availability:** The system has high-availability requirements and HIRTA's service level agreement (SLA) with the MOD platform and wayfinding solution vendors will govern the availability of their products. The SLA language focuses on the following key aspects of the system availability:
 - Definition of types of expected issues and their severity.
 - Identification of vendor response time and level of support to be provided depending on the severity of issue and the level of support needed, in the event an issue is reported.
 - Identification of key performance indicators (KPIs) with respect to system performance.
 - Guidance on planned system/data maintenance schedule.
 - Vendor support cost as applicable by the severity of an issue.
 - Clear description on what may constitute a maintenance update, system upgrade, or new enhancement, and what is covered per the vendor-agency contract.

- Identification of vendor credits as applicable in the event of a system outage /unavailability.
- Terms and conditions attached to the data breach or other security issues.
- Definition of roles and responsibilities (vendor, agency, third parties) with respect to system maintenance and incident response.

2.3 Data Security Requirements

Please see 'Safeguarding Methods and Processes' in Table 4, which discusses protections by data and dataset.

2.4 Risk Assessment of Threats

Because much of the data used to operate and to report on the performance of Health Connector will be produced and managed by the MOD platform vendor, this section reflects dataset risk assessment measures that align with the selected MOD platform vendor's abilities. In addition, it outlines assessment risk measures for surveys, healthcare appointment data, and wayfinding. The risk selection methodology emerged from a conversation with the MOD platform vendor, leading to the group's consensus that the risk likelihood for each dataset was deemed low. During this discussion, the Health Connector team explored distinctions between risk and impact, highlighting that something can pose low risk yet have the potential for significant impacts. More information on incident management can be found in the Incident Management Plan. For privacy purposes this plan will not be shared publicly.

Definitions of risks are provided below:

- **Very Low:** Probability is less than 10% and it is extremely unlikely that such an event would occur.
- **Low:** Probability is 30% and it is unlikely that such an event would occur.
- **Medium:** Probability is 50% and it is likely that such an event could occur.
- **High:** Probability is 70% and it is highly likely that such an event would occur.
- **Very High:** Probability is 90% and it is certain that such an event would occur.

Table 6. Dataset Risk Assessment

Dataset	Likelihood of Risk	Likely Impact	Mitigation
Admin	Very Low - Probability is less than 10% and it is extremely unlikely that such an event would occur.	Threats to the admin dataset could result in exposure of PII for Travelers.	MOD Vendor would follow up with a ticket and ensure issues are corrected as soon as possible.
Driver	Very Low - Probability is less than 10% and it is extremely unlikely that such an event would occur.	Threats to the driver dataset could result in exposure of PII for Drivers.	MOD Vendor would follow up with a ticket and ensure issues are corrected as soon as possible.
Trip	Very Low - Probability is less than 10% and it is extremely unlikely that such an event would occur.	Threats to the trip dataset could result in the exposure of PII for Travelers.	MOD Vendor would follow up with a ticket and ensure issues are corrected as soon as possible.
Aggregated	Very Low - Probability is less than 10% and it is extremely unlikely that such an event would occur.	Threats to the aggregated dataset are unlikely to result in impacts to daily operations and would primarily be disruptive to performance measurement.	MOD Vendor would follow up with a ticket and ensure issues are corrected as soon as possible.
Survey	Very Low - Probability is less than 10% and it is extremely unlikely that such an event would occur.	Threats to the survey dataset may result in the exposure of Traveler PII.	ISU is taking steps to ensure no PII beyond name and contact information is collected through surveys (no addresses or other sensitive information).

Dataset	Likelihood of Risk	Likely Impact	Mitigation
Healthcare appointment	Very Low - Probability is less than 10% and it is extremely unlikely that such an event would occur.	Threats to the health dataset are unlikely to result in impacts to daily operations but may result in the exposure of Traveler PII. PII does not include sensitive health data, but may include names.	Should any data breach occur, Flexlynqs will follow the Breach Response Plan, discussed in more detail in section 3.2.2.3. Epic, Veradigm, or other EHR partners have internal protocols that would also be followed in the event of a security breach and exposure of appointment data.
System log	Very Low - Probability is less than 10% and it is extremely unlikely that such an event would occur.	Threats to the aggregated dataset are unlikely to result in impacts to daily operations and would primarily be disruptive to performance measurement.	MOD Vendor would follow up with a ticket and ensure issues are corrected as soon as possible.
Wayfinding	Very Low - Probability is less than 10% and it is extremely unlikely that such an event would occur.	Threats to the wayfinding dataset are unlikely to result in impacts to daily operations and would primarily be disruptive to performance measurement.	N/A due to low risk and low impact

2.5 Data Sharing and Provision

As per the agreement with the MOD vendor, “Subject to the rights granted Contractor pursuant to this Agreement, all right, title and interest in and to the data, plans, schematics, or other documents collected and developed during the performance of this contract shall at all times remain the sole and exclusive property of HIRTA. Contractor shall surrender all such data to HIRTA prior to submitting an invoice for final payment. Contractor shall not claim any copyright or other restriction on or infringement of this transfer of intellectual property rights and shall deliver all such documents in hard copy and in electronic format specified by HIRTA.” The MOD platform’s Traveler app terms and conditions will reflect HIRTA’s privacy policy, which allows for the use of anonymized and/or aggregated data to be used for Health Connector performance evaluation and research.

The system is licensed to HIRTA. HIRTA will comply with all licensing regulations set forth in the agreement. This project incorporates several off the shelf licensing components as well as planned custom configurations and potentially new feature builds as an outcome of the project

pilot. The licenses will include licensing agreements from the MOD platform vendor, as well as other third-party vendors such as the wayfinding solution vendor.

Open data through the USDOT-managed system will be made available, as described in Table 3 and under a Creative Commons, Attribution License, [CC0](#). This license allows USDOT permission to publish the data submitted to the full public domain, allowing the public to copy, distribute, adapt and make use of the data submitted. Section [2.2.1 Public/Open Data](#) and section [2.2.2 Private Data](#) further describe the methods by which data will be made available.

Health Connector middleware code will be available through a public [GitHub repository](#) managed by Flexlynqs/Varasi, under a Creative Commons, Attribution License. Further details about the middleware can be found in the Middleware Design Document which will be appended in the SDD [7].

2.6 Specific System Hardware Security Analysis

2.6.1 Traveler Personal Device

Booking Health Connector rides will occur primarily through using applications on each Traveler's personal device. While each rider is responsible for their own device, security concerns arise should this device be lost or misplaced. If someone else were to come into possession of another Traveler's device while a user is still logged into the app, unauthorized individuals would be able to see past rides, appointments, payments, and personal information. This will be mitigated by having logins automatically time out after a designated period of time. Individual devices could also be vulnerable to cyber-attacks if networks are unsecured or if security is inadequate. However, this breach of security would be contained to individual information leakage and does not pose a threat to system-wide security. This type of security risk is to be managed by Travelers themselves.

2.6.2 Transit Vehicle On-Board Equipment

On-board transit equipment, such as driver tablets, used as part of Health Connector remain vulnerable to outside cyber-attacks if not protected properly. Drivers will be educated as to proper sign-on and sign-off procedures and all devices should be updated and protected as much as possible. In addition, tablets are often vulnerable to theft and will be safely secured to the bus and monitored by operators to ensure the system can continue running as intended.

2.6.3 HIRTA IT Hardware

The HIRTA TMS and Call Center have IT equipment, such as phones and computers, that are integral to the dispatching process. This hardware, like other transit operator hardware, is vulnerable to cyber-attacks such as ransomware or malware that can affect service systemwide. If such technology were affected, Health Connector would likely be unable to function or would have to rely entirely on third-party vehicles to provide service. As such, measures should be taken to ensure devices are secure and up to date. These measures may include proactive

cybersecurity protections such as firewalls, cryptography, physical security, and privacy preservation.

2.6.4 Access2Care and Health Partner IT Hardware

Access2Care, as well as partner healthcare institutions, also rely on independent hardware, such as computers and phones, to help Travelers use Health Connector. Access2Care manages trips for Medicaid Travelers, and health navigators help connect patients with healthcare providers and HIRTA (or other transportation service providers) by providing information and referral services. Associated hardware between these groups handles sensitive personal information and electronic health records and is also vulnerable if not properly protected. Proper measures should be taken to ensure devices are secure and up to date. Upon transition to MTM as the Medicaid broker, such measures will continue to be taken.

2.6.5 Wayfinding Kiosks

As Travelers navigate to their destinations, they may be aided by physical wayfinding kiosks in the field, primarily at healthcare facilities. These devices would show Travelers the way to their vehicles or to specific appointment rooms. Public-facing kiosks are generally unsupervised, making them easy targets for security breaches. In particular, security concerns may include kiosk settings being altered, people using the device to access inappropriate content, and vulnerabilities to cyber-attacks. Solutions will include locking kiosks into single-app mode, ensuring all software is up to date and networks are secure, and either remote or in-person kiosk monitoring to ensure proper use. In addition, kiosk tablets will need to be physically secured to a stand or otherwise locked in place to prevent them from being removed.

3 Security Controls

3.1 Technical Controls

3.1.1 Cybersecurity

3.1.1.1 MOD vendor

Cybersecurity controls have been established by the MOD platform vendor these include:

- Supplied applications shall provide secure data exchange via transport layer security/secure socket layer protocol (version 1.2 or higher).
- Supplied applications shall be digitally signed with established third-party certification authorities using methods appropriate to the targeted platforms.
- The system shall track and monitor all access and attempted access, including suspected threats to network resources, field devices, applications, and cardholder data.
- Vulnerabilities or exploits discovered by the Contractor or others shall be reported to HIRTA immediately (within 48 hours) with a proposed mitigation strategy and remediation plan with expected resolution dates.
- Application security shall be provided in accordance with best practices identified in the National Institute of Standards and Technology (NIST) Cybersecurity Framework or an equivalent alternative published standard from a recognized security-standards body, if approved by HIRTA.
- The Contractor shall inform HIRTA of any security breaches or data loss within 48 hours of discovery of the incident.
- The Contractor shall provide a detailed security incident response plan. The incident plan shall, at minimum, include the following:
 - Incident reporting process and how details of an incident will be communicated to HIRTA.
 - Incident reporting process and how the details of an incident will be communicated to the riders if deemed appropriate by HIRTA.
- Process for reporting vulnerabilities or exploits discovered by the Contractor or others and include at minimum a proposed mitigation strategy and remediation plan with expected resolution dates.
- The Contractor shall provide annual assurance statements of recertification and regulatory compliance delivered to HIRTA's Contract Liaison. The Contractor shall provide annual attestations of compliance program certifications relevant to the controls and security plan devised for the solution or system.
- The Contractor will share system security plan with HIRTA that includes processes for handling PII. The Contractor will comply with all relevant federal, state and local regulations and will only collect data that will improve the rider experience and would be needed for rider

support and rides investigation. Documentation on solution or system and Contractor's safeguards of the privacy of the following customer data shall be presented upon request:

- Description of all customer data in accordance with Federal, State, and Local regulations.
 - Statements of purpose for the collection of personally identifiable information (PII).
 - Description of data quality and integrity checks that provide for validation and verification of PII.
 - Description of data minimization and retention checks that ensure PII collected, used, and retained is relevant and necessary for the purpose for which it was originally collected.
- The Contractor shall provide notice of a loss or suspected loss of privacy sensitive data to HIRTA and HIRTA-designated users, within 48 hours of loss or suspected loss.

3.1.1.2 HIRTA

In the event of Health Connector reported vulnerabilities, exploits, and security incidents, HIRTA will share incident reports with USDOT.

3.1.1.3 NaviLens

For information on how NaviLens manages their data please refer to their [Privacy Policy](#).

3.1.1.4 Middleware vendor/Flexlynqs

Flexlnqs maintains extensive data security protocols through physical, technical, and administrative measures. Flexlynq's privacy policy can be made available upon request.

3.1.1.5 ISU

Data security is described in section [3.1.2](#). ISU does not have additional cybersecurity measures for data which are stored on the secure servers.

3.1.2 Data Security

3.1.2.1 MOD vendor

Please see Cybersecurity, MOD vendor section 3.1.1.1. Further data access requirements the selected MOD platform has agreed to comply with, include:

- All Contractor supplied applications shall support role-based security, allowing access to system functionality and data based on the roles of the users.
- The system shall have the ability to regulate access to functionality and access to data for authorized external or third-party users.
- The system shall record login, logout, and configuration change activities of all users from HIRTA and HIRTA-designated users.
- The activity log shall be accessible by authorized HIRTA system administrators for audit.
- Access control shall be configurable by HIRTA and its authorized system administrators.

3.1.2.2 *NaviLens*

NaviLens is ISO 27001 certified, the certificate cannot be published but can be made available upon request. For additional information on how NaviLens manages their data please refer to their [Privacy Policy](#).

3.1.2.3 *Middleware vendor/Flexlynqs*

Flexlynqs, along with software development partner, Varasi, maintains extensive data security protocols through physical, technical, and administrative measures. These specific protocols are not publicly available.

3.1.2.4 *ISU*

For all data analysis, ISU follows best practice data privacy standards. Data will be stored on CyBox which is a FERPA- and HIPAA-compliant file storage system. CyBox includes encryption of laptops and other devices that access the servers to minimize data breaches. Access to the surveys is through a multi-factor identification system. Remote access requires a VPN login. Survey data will be collected by ISU. Survey responses will also be stored in CyBox. Researchers will be required to have IRB approval in order to access the data. Researchers will be instructed to log off the system when not actively using/accessing data. A protocol will be established for security breaches (i.e., lost/stolen laptops, identity theft, data breaches). ISU will follow additional protocols as needed based upon the classification of the specific data type (HIPPA, ITAR, NIST 800-171, PCI, etc.).

3.1.3 Back-up and Recovery

3.1.3.1 *MOD vendor*

Vendors will use a highly reliable system and data environments will be designed to protect any data loss due to routine and ad-hoc maintenance processes that may require data back-up and recovery. Recovery requirements as outlined in the MOD vendor agreement include:

- The system and services shall maintain 99.9% availability as measured on a rolling monthly and annual basis, excluding pre-approved system maintenance down time and issues with networks provided by other Contractors.
- The Contractor shall test all updates, patches, upgrades, and configuration changes on Contractor's internal development environment prior to being implemented in the production environment. Reports of this testing shall be provided to HIRTA upon request.
- The Contractor shall provide provisions for HIRTA and HIRTA-designated users to test any updates, patches, upgrades, and configuration changes to the system before being implemented.
- The Contractor shall provide a disaster recovery plan highlighting how continued functionality can be provided in a disaster scenario (e.g., failover, fallback, recovery point objective [RPO], and recovery time objective [RTO]).

- Any system failover to support disaster recovery shall be completed within a recovery time objective (RTO) of one (1) hour.
- Any system failover shall be completed with a recovery point objective (RPO) of 1 minute.
- The Contractor shall set up the central system in redundant configuration by default.
- The system shall automatically switch to geographically redundant secondary (failover) site in case the primary site is unavailable. A secondary (failover) site shall be available when the system goes into revenue service.
- The system shall not lose any data when transitioning over from the primary to secondary site during a disaster induced failover or test, or when transition back from the secondary to primary site.

3.1.3.2 NaviLens

NaviLens is ISO 27001 certified, the certificate cannot be published but can be made available upon request. For additional information on how NaviLens manages their data please refer to their [Privacy Policy](#).

3.1.3.3 Middleware vendor/Flexlynqs

Flexlynqs, alongside software development partner, Varasi, maintain multiple cloud environments to back up production data. In the event of a catastrophic loss of technology, power, or physical infrastructure, services delivery can continue using with remote access to cloud resources.

3.1.3.4 ISU

ISU will utilize CyBox which is a FERPA- and HIPAA-compliant file storage system. CyBox includes a regular back-up so that data can be recovered. This includes the ability to access past versions of data in case of over-writes or data corruption.

3.2 Policy Controls

3.2.1 MOD vendor

HIRTA will be the owner of all datasets for the data collected within HIRTA TMS. Only authorized users, per their role, are provided access to specific modules of the system and the data generated by those systems, as identified in the system configurations. Except for those privileges, no user is authorized to make any changes. Also, the system audit trail shows if and what changes were made by a user.

ISU will only have access to anonymized and/or aggregated data and will retain the data for the full 7 years of the project. The MOD vendor will be required, through their contract with HIRTA, to also maintain the raw data for the full 7 years of the project.

3.2.2 NaviLens

Terms of use of NaviLens application will be as described in the conditions of use (<https://www.navilens.com/terms>). Also, privacy terms will be governed by Navi Lens privacy policy (<https://www.navilens.com/privacy>).

3.2.3 Middleware vendor/Flexlynqs

Relevant middleware data will be stored on network shares on Flexlynqs/Varasi-managed data shares and services. The use of personal or other non-Flexlynqs/Varasi managed assets (e.g., personal laptops, personal iPads, personal desktop computers) or personal or other non-Flexlynqs/Varasi managed services (such as online file storage, sharing, email or services) in each case is strictly prohibited. All production data along with backup copies of production data are to be stored on Flexlynqs/Varasi owned and managed external storage devices.

3.2.4 ISU

Only authorized users, per their role, are provided access to data. Except for those privileges, no user is authorized to make any changes or access to data. Additionally, a system audit trail shows if and what changes were made by a user.

3.3 Breach Plan

This section summarizes the action plan the site will take should there be a breach in data security.

3.3.1 MOD vendor

The Contractor shall inform HIRTA of any security breaches or data loss within 48 hours of discovery of the incident. Please see Cybersecurity, MOD vendor section [3.1.1.1](#). The Security Management Plan will not be published publicly but can be provided upon request.

3.3.2 NaviLens

NaviLens' breach plan as it relates to Health Connector will be determined upon the completion of contracting in Year 2 of Phase 2. NaviLens is ISO 27001 certified, the certificate cannot be published but can be made available upon request. For additional information on how NaviLens manages their data please refer to their [Privacy Policy](#).

3.3.3 Middleware vendor/Flexlynqs

Should a Personal Data Breach occur, Flexlynqs/Varai will follow the Breach Response Plan, which lays out in detail the roles and responsibilities of IT, general counsel as the data protection officer, marketing and communications, and human resources. A detailed cybersecurity plan may be made available upon request for security audits but is not available to be included in this public document.

3.3.4 ISU

Per ISU policy, if PII is inadvertently included in a response, it will be deleted, and those responsible for providing the data would be notified of the error. ISU will immediately report any security breaches to HIRTA and USDOT.

Appendix A. Acronyms and Glossary

Table 7. Acronyms

Acronym	Meaning
ADA	Americans with Disabilities Act
API	Application Programming Interface
APN	Access Point Name
BAA	Business Associate Agreement
CCB	Change Control Board
CSV	Comma-separated values
DCHD	Dallas County Health Department
DMP	Data Management Plan
DPP	Data Privacy Plan
EHR	Electronic Healthcare Record
FHIR	Fast Health Interoperability Record
GTFS	General Transit Feed Specification
GTFS-flex	General Transit Feed Specification for flexible and deviated-route transit services
HIRTA	Heart of Iowa Regional Transit Agency
HTTPS	Hypertext Transfer Protocol Secure
HL	Healthcare Lead
IP	Internet Protocol

Acronym	Meaning
ISU	Iowa State University
I&R	Information and Referral
IVR	Interactive Voice Response
JSON	JavaScript Object Notation
MOD	Mobility on Demand
NOFO	Notice of Funding Opportunity
PDF	Portable Document Format
PII	Personally Identifiable Information
PMESP	Performance Measure and Evaluation Support Plan
PML	Project Management Lead
PMP	Project Management Plan
REL	Research and Evaluation Lead
SAE	Society of Automobile Engineers
SDL	System Development Lead
SEL	Stakeholder Engagement Lead
SFTP	Secure File Transfer Protocol
SHP	Shape File Format
SPII	Sensitive Personally Identifiable Information
SSL	Secure Socket Layer
TCP	Transmission Control protocol
TDS	Transactional Demand Standard

Acronym	Meaning
TL	Technology Lead
TMS	Transportation Management System
UDP	User Datagram Protocol
UNIRP	User Needs Identification and Requirements Planning
USDOT	United States Department of Transportation
VAN	Vehicle Area Network
VOC	Via Operations Center
WAV	Wheelchair Accessible Vehicle
XML	eXtensible markup language

Table 8. Glossary

Term	Definition
Access2Care	A transportation broker for State of Iowa Medicaid program that performs booking and scheduling and works with service providers such as HIRTA for successful delivery of Medicaid-eligible trips.
Billing	Refers to the process of invoicing third-party funding sources (e.g., Medicaid) after a successful delivery of a trip. Billing is typically done on a monthly basis.
Cost Allocation	Refers to the process of associating a funding source that should be billed for a trip in a shared ride scenario when riders covered by separate funding sources share the vehicle for their trips and trip purposes at the same time.
Dispatching	Refers to an operations management function which involves assigning vehicle, tracking fleet location, managing schedule adherence, managing trip manifests and other operational functions.

Term	Definition
EHR/Medical Record System	Refers to the systems used by partner hospitals and clinics for booking medical appointments and maintaining their appointments, including discharge and any subsequent referral activities. Participating Healthcare partners currently use different EHR services. The following bullet points outline participating healthcare partners and the EHR systems they currently employ. Health Connector developed an interface with Dallas County Hospital, who currently uses Veradigm EHR and will transition to Epic EHR in the coming years. Other potential partner clinics for expansion include: • MercyOne Hospital – Epic EHR, Epic EHR provides a publicly available API • The Iowa Clinic. – Veradigm EHR
Health Navigator	Refers to services provided by Dallas County Health Department to Dallas County residents in identifying resources as necessary for improving social determinants of health.
Health Navigator and Healthcare End Subsystem	Refers to the limited access MOD platform that will be available to health navigators and healthcare customer care staff to request trips, modify trip requests, and check on trip status on behalf of Travelers. Additionally, health navigators and the health administrator at the Dallas County Health Department (DCHD) use a Microsoft Access-based information and referral (I&R) product to track the status of referral activities and for coordination with Dallas County residents' health navigation/social care services.
Information and Referral	Refers to public and private entities that help their customers in identifying resources for health and human services and other needs.
Medicaid Transportation Broker	Refers to the State of Iowa Medicaid broker. Currently, Access2Care's system is used for booking and managing Medicaid trips. HIRTA is one of the providers used by Access2Care. Medicaid trips will continue to be booked by Access2Care when requested by Travelers. Medicaid trips will be ingested in the HIRTA system when assigned to HIRTA. At that point, a Traveler using Medicaid benefits will be able to use Health Connector Traveler tools.
Middleware	Refers to an interface application that enables data exchange between two disparate systems or applications using API endpoints offered by those applications.
Provider	Provider in this context mainly refers to an entity performing service delivery for requested trips, sometimes also referred as service provider. The HIRTA team has also used healthcare partners as providers in some cases but referred as 'healthcare providers.'

Term	Definition
Reservation	Refers to the act of booking a trip based on a request from a Traveler. Reservation is available to only registered Travelers.
Scheduling	Refers to the process of identifying driver and vehicle resources and their runs/shifts for a given workday. Scheduling is typically performed for all requests received until 24 hours in advance. Booking within 24-hour notice and on-demand is offered but not encouraged due to limited system capacity and resources.
Smart Device	Refers to smartphone, smartwatch and similar personal devices that may be internet enabled and are equipped with sensors.
Traveler	While ‘customer’ is commonly used by transit agencies and ‘patient’ or ‘consumer’ by healthcare facilities, for this project (and in this document), ‘Traveler’ will be used to identify individuals who may benefit from Health Connector.
Traveler-end Subsystem	Includes the tools and technologies (phone/interactive voice response (IVR), mobile/smart devices, web-based tools) to be used by Travelers seeking transportation services for their healthcare appointments as part of their pre-trip, during trip, on arrival, and return trip activities. This includes both a mobility-on-demand (MOD) application for planning, booking, and payment, as well as a wayfinding application for more detailed guidance within care facilities. This application, provided by Via, also provides real-time status of trips on demand and through push notification services and allows Travelers to discover options and plans trips. Mobile/smart devices will be used as part of the Traveler-end subsystem but are not a part of this procurement.
Transportation Management Subsystem (TMS)	TMS refers to any systems related to the operational backend functions involved in service delivery. Under this project, The MOD TMS (also referred to as “VOC”) and the HIRTA TMS are commonly referenced as such systems.
Vehicle Subsystem	Refers to the technologies deployed on vehicles to support driver-end functions for driver-dispatch communications, manifest management, support just-in-time dispatching, turn-by-turn navigation and outdoor wayfinding (e.g., to locate Travelers at the time of pickup), on-board information and fare payments. On all HIRTA-owned vehicles, drivers will use tablets running the driver app. On other vehicles, drivers may use the driver app on their tablet or their phone.
Wayfinding	Refers to the tools and technologies that assist in orientation, locating objects, and step-by-step navigation to destinations in outdoor and indoor environments using visual markers, sensors, or physical signage.

Appendix B. References

1. Mishra, et al. (2021), *Data Management Plan (DMP) - Heart of Iowa Regional Transit Agency ITS4US Deployment Project (FHWA-JPO-21-867)* U.S. Department of Transportation.
2. Mishra, et al. (2021), *Concept of Operations (ConOps) - Heart of Iowa Regional Transit Agency ITS4US Deployment Project (FHWA-JPO-21-859)* U.S. Department of Transportation.
3. Mishra, et al. (2022), *Performance Measurement and Evaluation Support Plan (PMESP) Heart of Iowa Regional Transit Agency ITS4US Deployment Project (FHWA-JPO-21-877)* U.S. Department of Transportation.
4. Mishra, et al. (2022), *Systems Requirements Specifications (SyRS) Heart of Iowa Regional Transit Agency ITS4US Deployment Project (FHWA-JPO-21-882)* U.S. Department of Transportation.
5. USDOT (2022). *National ITS Reference Architecture v9.1 Security Analysis Methodology*.
6. Zeilinger, et al. (2022), *Human Use Approval Summary (HUAS) - Heart of Iowa Regional Transit Agency ITS4US Deployment Project (FHWA-JPO-21-897)* U.S. Department of Transportation.
7. Mishra, et al. (2022), *System Design Document (SDD) - Heart of Iowa Regional Transit Agency ITS4US Deployment Project*

Appendix C. User Groups

This table, initially represented in the Systems Requirements Document [4], has been expanded to include organizations and applications that will provide and access Health Connector data for project implementation and performance evaluation.

Table 9. User Groups

Organization	User Group	Abbreviation	Short Description
DCHD	Health Navigators	HNV	Refers to the employees of the Dallas County Health Department (DCHD) who connect customers/patients with healthcare providers and HIRTA (or other transportation service providers) by providing information and referral services.
DCHD	Health Administrator	HAD	Dallas County Health Commissioner (or individuals in similar role) responsible for wellbeing of the community. Users of the system for measuring performance and health outcomes.
HIRTA	Trip Scheduler	SCH	HIRTA staff who processes customer requests and schedules rides.
HIRTA	Transportation Operations Staff	OPS	HIRTA staff who assigns trips to vehicles, monitors trips, coordinates with drivers in real-time (e.g., their ability to perform additional trips, assisting to find origin or destination locations, help resolve no-show or cancellation) and makes reassignments if necessary. At times, this process may also be fully automated and performed by the dispatching algorithm (e.g., TNC that may be used as third-party provider for real-time trips include algorithm that does dynamic ride-matching with available driver pool without manual interaction).
HIRTA	Customer Service Staff	CSR	Refers to HIRTA customer service staff who responds to travelers' requests for all aspects of their trip experience beyond trip booking/cancellations.
HIRTA	Driver	DRV	Refers to HIRTA or contractor employees who pick up and drop off customers for their requested trips. There are no major changes expected for drivers as part of this implementation but relevant needs are documented.

Organization	User Group	Abbreviation	Short Description
HIRTA	Administration	ADM	HIRTA staff responsible for administrative functions such as verification of trip data, cost allocation, third-party billing (e.g., to funding sources), accounting and reporting. Most of this process will not change but certain flows are planned to be automated (e.g., interface with Medicaid).
Contractor	Third Party Service Provider	CTR	Refers to contractors that may work with HIRTA in the future to provide services when HIRTA does not have the capacity through its own fleet.
Healthcare Partner	Healthcare Customer Care Staff	HCR	Healthcare staff who take calls and intake customer request for medical appointments. Customer care staff may do other coordination related to medical appointments as well.
Healthcare Partner	Healthcare Operations Staff (e.g., customer care, nursing, community health partnership)	HOP	Staff that is responsible for interacting with customer on check-in and check-out. Also, includes staff that interacts with HIRTA, DCHD and other community partners on behalf of patients related to their appointments.
Healthcare Partner	Community Health Partner	CHP	Staff that interacts with HIRTA, DCHD and other community partners for improving experience for patients visiting healthcare facilities.
Other	Traveler	TRV	Individuals, who are HIRTA clients and are requesting transportation services for their medical appointments. These services may be performed using HIRTA-operated vehicles or through HIRTA contractors.
Other	Patients	PTN	Individuals who may not be HIRTA customers but are looking for transportation services for their medical appointments, referral appointments or follow-up appointments or other medical needs.
Other	Referral Agents	RFR	Individuals employed by organizations that connect the public to the providers according to their service requests. In this context services may be related to healthcare or transportation.
Other	Funding Entity	FND	Organizations funding customer trips (e.g., Medicaid) that will interface with the system for automated billing and payment processing. This includes Access2Care.
Other	Community Partners	CPS	Stakeholders representing underserved groups and will help identify needs for the groups they are representing. They will interface with the system for measuring performance of the system in meeting health outcomes within their communities
Other	Government Partner Agencies	GPA	Refers to local and state Government entities that partner with HIRTA and will help identify broad community-based needs (e.g., social determinants of health) and will use the system to stay informed on project outcomes
Other	MOD system	MOD	Refers to the MOD platform and supporting vendor staff.

Organization	User Group	Abbreviation	Short Description
Other	Wayfinding system	WAY	Refers to the wayfinding system and supporting vendor staff.
Other	Iowa State University	ISU	Refers to Iowa State University's Institute for Transportation (InTrans) and supporting staff.
Other	USDOT	USDOT	Refers to the USDOT-managed public data portal.

U.S. Department of Transportation
ITS Joint Program Office-HOIT
1200 New Jersey Avenue, SE
Washington, DC 20590

Toll-Free "Help Line" 866-367-7487
www.its.dot.gov

FHWA-JPO-22-971



U.S. Department of Transportation