Center for Medical Interoperability

TOGETHER for PPE Governance Policy

Edition 1.1

November 2019

Prepared by The Center for Medical Interoperability

8 City Boulevard, Suite 203 Nashville, TN 37209

(615) 257-6400

www.c4mi.org

Trademarks

Disclaimer

Document Lifetime

C4MI reserves the right to revise this document for any reason including, but not limited to, changes in laws, regulations, or standards promulgated by various entities, technology advances, or changes in equipment design, manufacturing techniques, or operating procedures described, or referred to, herein.

The Center for Medical Interoperability
Trust Platform Governance Plan, Edition 1.1

Authored by The Center for Medical Interoperability
Published by The Center for Medical Interoperability, November 2019

Table of Contents

1. Introduction *4*

1.1 Scope and Governance Principles **4**

1.2 Governance Mechanism **4**

2. Oversight *5*

3.1 Center for Medical Interoperability Trust Platform Governing Authority **5**

3.2 TOGETHER for PPE Steering Committee **5**

3. Administration of the Trust Platform *6*

3.1 Principles of Administration **6**

3.2 Duties of C4MI Trust Platform Governing Authority **6**

3.2.1 Requirements 6

3.2.2 Terms of Notification 7

3.3 Obligations of Trust Platform Participants **7**

3.4 Use of The Trust Platform **8**

3.4.1 Affiliation to Trust Platform 8

3.4.2 Refusal of affiliation application 8

3.4.3 Requirements for a data service 9

3.4.4 Provision and use of a data service 9

3.4.5 Termination of Trust Platform participation 9

1. Introduction

1.1 Scope and Governance Principles

This Charter and Governance document defines the policies, processes, and mechanisms governing the Trust Platform for the TOGETHER for PPE project. It establishes the Center for Medical Interoperability ("C4MI") as the governing authority of the Trust Platform and a Steering Committee specific to the TOGETHER for PPE project.

TOGETHER is a public-private partnership between C4MI and the Centers for Disease Control and Prevention ("CDC") to improve nationwide readiness and response. TOGETHER for PPE readiness is intended to address personal protective equipment (PPE) shortages during pandemics of highly infectious diseases. C4MI's Trust Platform for data exchange is uniquely suited to address interoperability gaps in information systems such as inventory management.

A uniform and foundational approach to Trust Platform governance and technical architecture promotes consistency in structure, specification of context through use cases, and supports reusability and modularity of the overarching architecture. To the extent possible, the Trust Platform is governed by the application of "Trust Characteristics and Requirements" that are detailed and specified in C4MI Healthcare Trust Platform Technical Architecture Technical Report (CMI-TR-HTP-WIP-06-20190906).

Together, these governing authorities provide strategy, process and mechanisms that will support trusted, secure, interoperable exchange of healthcare information across geographies, ecosystem participants, and existing information network relationships using different data sharing networks.

The Trust Platform supports a collaborative process among industry and government to facilitate consensus and develop the essential elements needed to allow this widespread connectivity. Organizations that elect to engage in exchange activities through the Trust Platform Technical Architecture will execute a Common Data Usage Agreement and will be able to interoperate with all other Participants and avoid the need to join multiple data exchange networks and execute several point-to-point policy agreements.

1.2 Governance Mechanism

The governance mechanism of the Trust Platform Technical Architecture consists of:

- Center for Medical Interoperability Trust Platform Governing Authority
- Center for Medical Interoperability TOGETHER for PPE Steering Committee Charter
- Center for Medical Interoperability Common Data Usage Agreement
- Healthcare Trust Platform Technical Specifications
- Trust Platform PPE Application
- Trust Platform HTP Implementation Guides

2. Oversight

3.1 Center for Medical Interoperability Trust Platform Governing Authority

C4MI is the Governing Authority of the Trust Platform and its role is to administer its use which includes, but is not limited to: managing change requests, new additions, and associated constraints to the Trust Platform. It is also responsible for documenting updates associated with each edition of the Trust Platform Technical Specifications, Trust Platform Common Data Usage Agreement, PPE Application, and HTP Implementation Guides.

3.2 TOGETHER for PPE Steering Committee

The role of the TOGETHER for PPE Steering Committee ("Steering Committee") is to serve as a primary resource and leadership team that guides C4MI Trust Platform activities as it relates to TOGETHER for PPE readiness project deliverables. The Steering Committee will guide and inform decisions related to the deployment of the Trust Platform for the TOGETHER for PPE project.

The Steering Committee will assist C4MI in managing and executing TOGETHER for PPE Common Data Usage Agreements with eligible participants.

Please refer to the Center for Medical Interoperability TOGETHER for PPE Steering Committee Charter for more detailed information.

3. Administration of the Trust Platform

3.1 Principles of Administration

The following main principles shall be observed in administration of the Trust Platform:

1) **Independence from the platform and architecture** – The Trust Platform enables a participant on a software platform to communicate with a data service provider on a software platform through the information system;
2) **Multilaterality** – A participant can apply for access to any data services provided through the Trust Platform;
3) **An open and standardized approach** – If possible, international standards and protocols are used in administration and development of the Trust Platform;
4) **Security** – Data exchange through the Trust Platform shall not alter the integrity, processability, and confidentiality of the data.

3.2 Duties of C4MI Trust Platform Governing Authority

3.2.1 Requirements

C4MI shall:

1) Administer the information of Trust Platform participants, security servers registered in the Trust Platform, and in the subsystems subscribed to The Trust Platform, in the production as well as test environment. This organizational structure will ensure the availability of the information required for generation of a secure Trust Platform data exchange channel and use of data services for the security server of a Trust Platform participant;
2) Organize processing of participants, subsystem, and security server applications;
3) Develop the terms and conditions for subscription to the Trust Platform and its applications and use;
4) Ensure access to use of the Trust Platform;
5) Monitor the use of the Trust Platform and collect usage statistics;
6) Handle any security incidents;
7) Notify Trust Platform participants of any changes in the administration or use of the Trust Platform, and of any circumstances or maintenance works restricting the use of the Trust Platform by sending e-mails to the contact persons of Trust Platform participants specified in the administration system of C4MI.
8) Administer and organize connection of the Trust Platform instance to other data exchange instances, if appropriate;
9) Ensure access to standardized security server software for Trust Platform participants;
10) Ensure the conformity of standardized Trust Platform solutions designed for end users of the data service with Trust Platform message protocol and access to the software for Trust Platform participants;

11) Prepare and implement development projects of Trust Platform infrastructure and ensure the architectural integrity of the Trust Platform;
12) In appropriate cases, suspend the availability of the information required for using a data service to the security server of a Trust Platform participant;
13) Administer and develop the solutions required for registration of participants and trust services to ensure functional operations and monitoring of the Trust Platform.

3.2.2 Terms of Notification

C4MI shall observe the following terms for advance notice:

1) Advance notice shall be given of any changes in the administration or use of the Trust Platform, and of scheduled maintenance works;
2) A minimum of 1 month of advance notice shall be given of any changes in the base protocol of the Trust Platform or in the Trust Platform message protocol, which call for change in the subsystem or data service of a Trust Platform participant.
3) In the event of extraordinary changes in the administration and use of the Trust Platform, and unscheduled maintenance works, C4MI shall have the right to observe shorter notice periods than specified in clauses 1 and 2) of this subsection;

3.3 Obligations of Trust Platform Participants

The participants of the Trust Platform are committed to keeping their information systems up to date and reliable

1) to ensure, upon joining the Trust Platform, the continuity, management and development of its information system as well as secure and trouble-free operation so that other participants can reliably exchange data with it;
2) to keep company information updated with the administration systems of the governing authority (C4MI);
3) to forward Trust Platform related requests and other information to the governing authority.

To address and manage security risks, the participants of the Trust Platform

1) take data protection measures and appropriate physical, organizational and IT security measures to ensure the integrity, confidentiality and availability of data;
2) confirm compliance with information security requirements upon joining by executing the Trust Platform Common Data Usage Agreement;
3) provide, at the request of the governing authority, the information necessary for assessing the security of the Trust Platform, including the security rules and a description of the implementation of the measures implemented;
4) to provide and use data services in accordance with the TOGETHER for PPE Common Data Usage Agreement. The Common Data Usage Agreement shall specify
    a. the information security measures required for the use of the data service and the organizational, physical and IT security requirements for the subscriber of the data

service, taking into account the composition of the data to be processed and the requirements of the law;

b. service level terms.

5) determine the jobs and posts authorized to use the subsystem and thereby the data services made available by the subsystem, and restrict access within the organization to authorized persons only;
6) to notify the governing authority immediately of any problems and circumstances which affect or may affect the governing authority or a Trust Platform Participant in the performance of its duties. In addition, the Trust Platform Participant shall immediately inform the governing authority of security incidents and the imminent threat thereof;
7) should follow the guidelines for the safe use of public cloud services when hosting an information system.

To make data services accessible, all Trust Platform participants shall

1) register the data service with the Trust Platform infrastructure;
2) verify, prior to entering into any agreement with the data service user, that the data service user has adequate organizational, physical and IT security measures in place, including the legal status of the participants and participants of the connected environments;
3) ensure that the access rights of the Trust Platform system conform with the agreements between participants to use the data service. The use of the data service is possible in the subsystems of the Trust Platform participants that have been granted access rights to use the specific data service;
4) Comply with the data service agreement;

3.4 Use of The Trust Platform

3.4.1 Affiliation to Trust Platform

1) Applications for affiliation to the Trust Platform shall be filed through C4MI.
2) Upon affiliation to the Trust Platform, the applicant shall enter into a Trust Platform Common Data Usage Agreement with C4MI. The affiliation agreement shall specify the parties' rights, obligations, and liabilities.

3.4.2 Refusal of affiliation application

C4MI shall have the right to reject an affiliation application to Trust Platform if:

1) The applicant has no unique identifier for which C4MI could issue a certificate in compliance with the requirements of C4MI;
2) The applicant has failed to submit the documents required for verification of the right of representation requested by C4MI or the applicant has no right of representation for submitting such application;
3) The applicant's details submitted upon affiliation are not registered with C4MI or the details are not up-to-date;

4) The applicant or the applicant's information system fail to meet other requirements specified in this Regulation or the principles of functioning of the Trust Platform.

3.4.3 Requirements for a data service

A data service shall:

1) Correspond to the Trust Platform message protocol and Data Exchange Policy established by C4MI;
2) Be registered in C4MI database with an updated and relevant description meeting the requirements set by C4MI and include information about the security measures required to use the service, taking into consideration the composition of the data included in the data service and the nature of the data service;
3) Be usable in the Trust Platform test environment.

3.4.4 Provision and use of a data service

1) Data services shall be provided and used pursuant to the contracts for using data services entered into by Trust Platform participants.
2) The data service provider shall:
    a. Verify prior to entry into a contract with a data service client whether the data service client is applying sufficient measures to ensure the integrity, confidentiality, and processability of the data to alleviate security risks;
    b. Ensure that Trust Platform access rights conform to the contract for using the data service entered into by Trust Platform participants.
3) Data services can be used in the subsystems of Trust Platform participants, for which access rights for using a specific data service have been granted.
4) Data service clients and providers shall:
    a. Follow the contract for using the data service;
    b. Timestamp all messages.
5) Trust Platform participants shall ensure, through their information system, authentication and authorization of the end user participating in the provision or using of a data service.

3.4.5 Termination of Trust Platform participation

1) A Trust Platform participant may terminate the participation at any time by filing a respective written application to C4MI.
2) In the event that the termination application does not contain the date of termination of the Trust Platform participant, the participant shall be terminated as of the working day following the date of receipt of the above-mentioned application.
3) C4MI shall have the right to terminate a participant with immediate effect or restrict the rights arising from the participation or issue a deadline for elimination of a deficiency if:
    a. a Trust Platform participant violates the terms or conditions specified in this Regulation or in the procedure of data service hosting;
    b. a Trust Platform participant has filed incorrect or incomplete data.
4) C4MI shall have the right to terminate a participant by notifying the Trust Platform participant thereof by e-mail 30 calendar days in advance in the event of a failure of the Trust Platform participant to respond to repeated inquiries issued by C4MI.