# Trust Framework System Rules for Personal Data and Individual Identity Services

# Preface

This document provides Trust Framework System Rules[[1]](#endnote-1) for the provision of Personal Data and Individual Identity services. The architecture and model followed by these System Rules enables interoperability at the business, legal and technical dimensions, and ensures that each of those dimensions is expressly aligned, harmonized and integrated. The higher level and implementation agnostic “Model Rules[[2]](#endnote-2)” can be found at <http://ecitizen.mit.edu/ModelRules>

Specifically, these System Rules anticipate and are tailored to support a prospective production grade roll out of OpenPDS and FUNF software for Reality Mining and more generally as an example of how System Rules following this model can enable and accelerate achieving the broader goal of a Personal Data Ecology. Please note that for purposes of presenting a complete and coherent reference example, “placeholders[[3]](#endnote-3)” and “hooks[[4]](#endnote-4)” have been used when names of parties or business services. For future commercial or production grade use of these Rules, implementers would replace the example parties, service descriptions, etc, with the respective applicable names or terms.

# 1. BUSINESS RULES[[5]](#endnote-5)

1.1 Scope and Purpose

These System Rules apply to the use of the Personal Data and Individual Identity System by Individual Users, Third Party Providers and the System Provider, individually and in any combination. These System Rules are intended to enable individuals to

1.2 Intended Context and Scenario of Use[[6]](#endnote-6)

The intent of these System Rules is to provide a method to ensure the purpose the System is reliably and efficiently enabled. The focus of these Rules is to standardize essential interface and interoperability implementation requirements necessary to ensure expected outcomes by all Parties while encouraging wide latitude for individually agreed interactions and competitively evolving innovation.

1.2 Parties and Roles

These System Rules are applied by and to the following Parties, as per each such party’s contractual assent to the Terms of Agreement for participation in the System and agreement to comply with the relevant provisions of these System Rules including acceptance of the rights, obligations and functions allocated to the Role or Roles agreed by each Party:

1.2.1 Individual User

An individual human being who has contractually assented to Terms of Agreement and is a customer holding a valid account with the Personal Data Store. An Individual User may use their account to request, accept and use a Grant of Authorization to access the Personal Data of a Principal Individual User.

Any individual human who contractually assents to the Terms of Agreement is eligible to apply for and hold an Account on the System. Services or other premium functions offered on a subscription, one time fee or other billing basis are available subject to fulfillment of applicable payment terms as agreed by the Individual User.

The individual human beings that are indicated on the then current records of “Individual Users” at the System Registry.

1.2.2 Principal Individual User

An individual human who has contractually assented to Terms of Agreement and is a customer holding a valid account with the Personal Data Store. An Individual User may use their account to store their own Personal Data on the System and to Grant Authorization for accessing that Personal Data to Third Party Service Providers and/or to Individual Users.

1.2.3 System Provider

The Party or Parties responsible for the Personal Data System, comprised of the Personal Data Store and Services. The System Provider promulgates these System Rules.

As reflected by the current record of System Provider in the System Registry: “Acme Personal Data Store, LLC, at: [URL would be inserted here, e.g. OpenPDS.com]” is the Party performing the Role of System Provider under these Rules.

1.2.4 Third Party Service Providers

The Party or Parties that operate and provide Third Party Services approved for use with the System and in accordance with these Rules. Only Third Party Providers that have been approved by the System Provider and contractually assented to Terms of Agreement are eligible to Participate in the System. To be eligible for approval by the System Provider, a prospective Third Party Provider must submit a Third Party Provider Application, including truthful, accurate and complete information. Every Third Party Provider must contractually assent to abide by and in practice adhere to these Rules. Any approved Third Party Provider may accept Individual User Grants of Authorization for access to that User’s Personal Data stored within or subject to access control by the System. Any approved Third Party Provider may establish such additional terms of service including with respect to billing, liability and service quality, with Individual Users of the System as the parties may agree provided that no contractual term or other obligation shall be enforceable against any Individual User to the extent the obligation arises from or applies to that User’s Grant of Authorization to the Third Party Provider and is inconsistent with any provision of these Rules.

To ensure the purpose of this System and expectations of Individual Users are met, every Third Party Provider must effectively implement the OAuth 2.0 System Approved Scopes and corresponding obligations and stipulations for each such Scope, including explicit agreement to accept enforcement of such obligations and stipulation by each Account Holder that has Granted such Authorization to the Third Party Provider. Failure to comply with these requirements renders any Third Party Provider ineligible for Participation and subject to termination, suspension or a review process at the sole discretion of the System Provider.

The entities that are indicated on the then current records of “Third Party Providers” at the System Registry.

1.3 System Services

1.3.1 Service Lifecycle

Approval by the System Provider is required as a precondition to the offering of any Service though this System. Any approved Service that is currently offered through the System is enumerated in Rule 1.3.2 and is available in accordance with the technical specifications defined under Rule 3.2 and subject to all relevant Rules and used subject to the relevant provisions of the Terms of Agreement of any Participant using the Service.

1.3.2 System Service

The following Services are approved and provisioned for use by or with the System, subject to these Rules:

1.3.2.1 "Personal Data Storage and Archive" services,

1.3.2.2 “Federated Identity” services,

1.3.2.3 “Personal Data Collection and Import” services,

1.3.2.4 "Personal Data Sharing Control" services,

1.3.2.5 “ Analytics and Visualization" services, and

1.3.2.6 “Personal Data Export and Deletion” services.

1.4 Recording and Reporting

Any Recording or Reporting requirement under these Rules, including within a Service Schedule or Specification must result in the logging of the required record at the System Registry within the time prescribed or if no time is prescribed or if allowed extenuating circumstances require a longer period of time then as soon as practicable. Any Core Legal Event must be logged with the System Registry immediately upon it’s occurrence.

1.5 Use of System Logo and Marketing

Any use of the System Logo, and any marketing, advertising or other public communications referencing approved Third Party Provider status or other affiliation with this System is prohibited unless explicitly permitted in the applicable Terms of Agreement and only for such time as the Terms of Agreement as in effect.

# 2. LEGAL RULES

2.1 Scope and Application

2.1.1 Promulgation of Rules

The content comprising the “System Rules” duly promulgated by the System Provider in accordance with these Rules, as published at [URL] is the formal and binding normative version of these Rules as of the moment of publication and until the moment of publication of a subsequent version or for such period of time as provided under these Rules.

2.1.2 Order of Precedence

In the event of a conflict between the provisions of these Rules and the provisions of the Terms of Agreement between any Parties to these Rules, then the provisions of these Rules shall prevail.

In the event of a conflict between the terms these Rules and an Independent Commercial Contract between any Parties to these Rules, then, as between a Principal Individual User and a Third Party Service Provider, the provisions of the applicable Terms of Authorization incorporated by reference into the Parties Terms of Agreement shall prevail, and otherwise the provision of the Independent Commercial Contract shall prevail other than

2.2 Rights and Obligations of Participants

2.2.1 General Obligation

All Participants agree to abide by the terms and act in accordance with these Rules and adhere to respect each Principal Individual User’s ownership and control rights to their own Personal Data stored in or accessible through this System.

2.2.2 Protection and Promotion of Individual Member Identity and Data Rights

The System Provider is responsible for safeguarding the Individual Principal User’s elemental rights to their own Individual Identity and ownership of their Personal Data and may as appropriate protect and defend such rights and as needed represent the interests of such User’s vis-a-vis external parties when such rights are threatened.

2.2.3 Minimum Required Obligations of Third Party Provider to Individual Users

Each Third Party Provider agrees to comply the Terms of Authorization between itself and each Individual User from whom the Third Party Provider has received a grant of authorization for access to personal data of such user, or use of the Individual User’s federated identity credential or other identity attribute. Specifically, notwithstanding any terms to the contrary in Third Party Provider’s terms of service, privacy policy of other contract, the promises and other assertions made to each User as is in association with each Scope type

2.3 Core Legal Event Verifiable Evidentiary Records

The Required Record of any transaction or other action subject to a Reporting requirements under Rule 1.4 or otherwise required under these Rules must be logged with the System Registry at [URL] and a copy preserved by the Third Party Provider independently in accordance with applicable Records Management requirements. Core Legal Events include at a minimum addition, change or de-provision of a System Service, the current Participants and any Change to these Rules, as well as each Grant of Authorization by a Principal Individual User.

2.4 Liability and Indemnification

Under these Rules, no Individual User shall be liable to nor shall owe any obligation of indemnity to any other party for any actions that were conducted in compliance with these Rules. The applicable provisions of the Terms of Agreement regarding liability, indemnity, damages and warranties shall apply to Parties to such agreements, subject to the Order of Precedence defined in Rule 2.1.2.

2.5 Intellectual Property

2.5.1 Trademark and License in System Trustmark and Logo

Use of the System trademarks or logos must comply with the Trustmark and Branding Policy and License Agreement. No Party may use or display any trademark or logo without explicit permission and license to do so. Parties that are engaged in a process of applying for participation are not parties to the License Agreement and not permitted to use such trademarks or logos. Parties that were Participants at one time but whose Participation status is suspended or terminated, whether voluntarily or involuntarily, are likewise not permitted to use or display the System trademarks or logos, and must cease any use that had previously been permitted in accordance with the license terms.

2.5.2 Copyright and License in System Rules

These Rules are available to be downloaded, stored, transmitted and duplicated on a royalty free, perpetual and global basis. The System Provider shall ensure an appropriate Creative Commons license or such other license as it deems appropriate is properly applied to these Rules. These Rules are an allowed derivative work of the MIT Model System Rules, available at <https://ecitizen.mit.edu/ModelRules>

2.6 Amendment

These Rules may be amended from time to time by the System Provider in accordance with the Notice requirements of Section 2.7.

2.7 Notice

Amendment of a Rule or change to the System that is not material is effective when duly promulgated by the System Provider and when both posted at [URL] and registered as a Core Legal Event to the System Registry. An affected Participant is entitled to receive 30 days advance notice of any amendment of a Rule or change to the System that constitutes material change, unless an emergency condition requires a shorter period or no notice.

2.8 Other Legal Terms

The Terms of Agreement, including the Terms of Authorization, as executed or adopted by each Participant include more specific terms and may include varying provisions, subject to Rule 2.1.2 governing Order of Precedence. The terms defining and governing the overall business relationship and legal rights, expectations or other responsibilities and duties of the Participants are addressed in one or more Independent Commercial Contracts executed or adopted by Participants, subject to Rule 2.1.2.

# 3. TECHNICAL RULES

**3.1 Scope and Application**

3.1.1 System Interface and Functional Implementation[[7]](#endnote-7)

The authoritative System Interface and Target Operating Implementation Model is published at: [URL] and describes the implementation, profiles and configurations of supported standards necessary to interoperate with the System at the services, transactions, messaging and protocol layers, including specification of REST and other API functionality.

3.1.2 Supported Standards

The System supports and depends upon the following Standards and relies upon conformance with and interoperability based upon correct implementation of these standards:

3.1.2.1 OAuth2

The System Authorization and Resource servers support the final version of the AUth2 Core as defined at <http://tools.ietf.org/html/draft-ietf-oauth-v2>

The System Authorization and Resource servers support the final version of the AUth2 Bearer Token usage as defined at Bearer: <http://tools.ietf.org/html/draft-ietf-oauth-v2-bearer>

3.1.2.2 OpenID Connect

The system supports and implements OpenID Connect as defined at <http://openid.net/connect>

The System OpenID Connect server supports the final version of the OpenID Connect protocol as defined at <http://openid.net/connect> Protocol Profile.

The System OpenID Connect server supports the following flows and options:

• Basic client profile (code flow) as defined by <http://openid.net/specs/openid-connect-basic-1_0.html> including:

- Authorization Code flow

- UserInfo Endpoint with "openid" schema

- Asymmetrically signed id\_token (with RSA)

• Additionally, the System OpenID Connect server supports the following optional components of OpenID Connect:

- Asymmetrically signed Request Objects (via RSA)

- Server keys published via JWK and X509

- Access tokens signed with RSA by server

- Dynamic client registration

- Server discovery

3.1.2.3 Claims

The following claims are supported from the UserInfo Endpoint with semantics defined in <http://openid.net/specs/openid-connect-messages-1_0.html>

• user\_id, guaranteed unique and stable per user

• name

• given\_name

• family\_name

• preferred\_username

• email

• email\_verified

• phone\_number

3.1.2.4 Authoritative Normative Sources

OpenID Connect:

Basic client profile: <http://openid.net/specs/openid-connect-basic-1_0.html>

Messages (abstract structure): <http://openid.net/specs/openid-connect-messages-1_0.html>

Standard (http binding): <http://openid.net/specs/openid-connect-standard-1_0.html>

Discovery: http://openid.net/specs/openid-connect-discovery-1\_0.html

Dynamic Client registration: <http://openid.net/specs/openid-connect-registration-1_0.html>

SWD: <http://tools.ietf.org/html/draft-jones-simple-web-discovery>

OAuth2:

Core: <http://tools.ietf.org/html/draft-ietf-oauth-v2>

Bearer: <http://tools.ietf.org/html/draft-ietf-oauth-v2-bearer>

JSON Object Signing and Encryption:

JWT (tokens): <http://tools.ietf.org/html/draft-ietf-oauth-json-web-token>

JWS (signing): <http://tools.ietf.org/html/draft-ietf-jose-json-web-signature>

JWE (encryption): <http://tools.ietf.org/html/draft-ietf-jose-json-web-encryption>

JWK (keys): <http://tools.ietf.org/html/draft-ietf-jose-json-web-key>

JWA (algorithms): <http://tools.ietf.org/html/draft-ietf-jose-json-web-algorithms>

3.1.3 Transactional and Core Records Registration

The authoritative records of any Core Legal Events, and any other records required to be Registered under these Rules must be submitted by the Participant owing the duty of Registration to the designated Registry, including:

Financial Records, Legal Contracts or Dynamic Grant Based Terms of Contracts and Technical Logs required to be Registered under these Rules; and Registration and Audit Logs required to be Registered under these Rules.

**3.2 Service Provision and Interface[[8]](#endnote-8)**

Services offered through the System are enumerated in Rule 1.3. The information and format necessary to describe the Service Schedule and Interface Specification applicable to a Service is available at [URL].

3.2.1 Federated Identity services

The System issues OpenID Connect compliant federated identity credentials to Principal Individual Users. The System accepts for purposes of Login and Account Identifiers externally issued OpenID Connect federated credentials that are issued in accordance with these Rules and that have been issued by Identity Providers that have approved by the System Provider.

3.2.3 Personal Data services

A Principal Individual User may import Personal Data and other records to their Personal Data Store that is hosted at the OpenPDS operated by System Provider by use of a Third Party Providers that has an approved service for that transaction.

3.3 Authorization and Permission Specifications

Only requests for access to Personal Data that conform with the defined Approved Scopes and Grant Types listed at [URL] are permitted or supported under these Rules.[[9]](#endnote-9)

3.3.1 Registered Clients and Services

For purposes of any transaction or other interaction that necessarily requires or will creates a Core Legal Event, the System must only accept an OAuth 2,0 or OpenID Connect request from a Party that has duly Registered as a Third Party Service Provider through the Manual Client Registration and Third Party Provider Application process and therefore is included on the Approved List of Parties, Services and Transactions. Reliance upon dynamic registration is not supported outside of the process of approval by the System Provider.

3.3.2 Core Legal Records

The applicable Required Record must be duly created and managed when any transaction or other action subject to a Reporting requirement under these Rules occurs with or by a Third Party Provider. Every Third Party Service must be implemented so as to ensure accurate, timely and accessible Required Records such that upon review an objectively verifiable account can be made of the relevant transactions or other actions, the salient terms (i.e. the data accessed, modified or deleted or other essential terms) the parties involves, the relevant times and the applicable Terms of Agreement and Terms of Authorization.

The format and data models required for Core Legal Records are published at [URL].

3.3.3 Registration and Reporting

Registration of Core Legal Records must be accomplished by any Third Party Service Provider obligated to Report by logging such Record with the System Registry in accordance with the Registraton and Logging Specification, published at [URL].

3.3.4 OpenPDS

The authoritative version and build of OpenPDS software supported and implemented in the System under these Rules is documented at [URL].

3.3.5 Core Apps

The Mobile Health FUNF App is a Core App available for use by Principal Individual Users. The specifications of the current supported version and build of this App and links to documentation is available at: [URL].

3.4 Security and Resilience[[10]](#endnote-10)

Passwords: Only an Principal User’s Account password can decrypt that user’s Personal Data or other sensitive information, and System Provider does not store this password. As a result, no one—not even System Provider employees—can see the sensitive information a Principal User places in the System. If a Principal User forgets his or her password and needs to reset it, the System Provider shall delete that user’s sensitive information for his or her own protection. System Provider must also have mechanisms in place to stop brute force attacks on passwords, and offer multi-factor authentication and secure password recovery

Servers: Personal Data is stored in a major U.S. server storage facility that has 24/7 security guards and biometric security for entry, has been issued an SSAE16 Type II SOC 1 Report, is a PCI Security Standards Council Member, is Safe Harbor Certified, and offers protection via firewalls, its own intrusion detection systems, and other measures.

Data Storage: All sensitive information is encrypted in Sysem database servers, including by the use of 256-bit AES encryption and RSA 2048 asymmetric key encryption. Personal Data containing sensitive information must be encrypted uniquely, in order to add an extra layer of security. Non-sensitive information may only be accessed through a Principal User-chosen password that must not be stored by the System Provider. While technically possible for a small and limited group of System operations employees to access non-sensitive information, they are strictly forbidden from doing so, consistent with System Provider policies and these Rules, unless required by law, and access to System Provider servers is carefully logged.

Secure Coding and Data Management Practices: System Provider shall not use insecure third-party delivery networks, and must ensure that Principal User Personal Data is never exposed. To that end, use of POST rather than GET requests, and other appropriate measures must be used to prevent such exposure. System Provider is not permitted to see Principal User Personal Data even in the context of crash reports. In addition, System Provider must not use data de-duplication methods, which can raise security and privacy concerns.

Security Testing and Certificates: System Provider conduct audits of System security, including penetration testing by outside firms. System Provider uses SSL certificates from VeriSign and GeoTrust. In addition, System Provider constantly monitors the System for potential threats and vulnerabilities.

Principal’s Control Their Personal Data: Only an Account Holder can grant individuals, companies or applications access to his or her Personal Data and permanently delete or export their Personal Data. Third Party Providers are not allowed to track Principals while they are on the System, and the System Provider does not track Principals when they leave the System or a mobile app that is part of the System.

System Provider Employees: All System Provider employees undergo background checks going back 10 years as a condition of employment, and all technical employees receive security training.

3.5 Testing and Change Management

The System makes available a sandbox and test harness to Third Party Provider applicants to test the readiness for business, legal and technical interoperability with other Participants and for Participants to text readiness of modified or new Services, Transactions or other functions. The testing environment and Change Management Policy is documented at [URL].

1. # Commentary

   These System Rules provide a model for future production grade roll out of the Personal Data Store and related services developed by the MIT Media Lab’s Human Dynamics group. The approach of the System Rules is intended to enable the use of the Android FUNF and OpenPDS software to collect and share behavioral information effectively while ensuring best practices for privacy protection and user-centered control and consent for sharing of personal data. The System Rules cover the roles, relationships, rights and responsibilities of parties who are individual users of the OpenPDS software and services and parties that provide the Personal Data Store as well as additional approved third party providers of services or apps.

   The approach is designed to be extensible to include additional types of technologies and services without need to change the basic model or method for using the Rules and therefore to be useful for future evolution of the PDS and FUNF software as well as for the reality analysis and personal data ecology research and development work of the MIT Media Lab Human Dynamics group more generally.

   Please note that for purposes of presenting a complete and coherent reference example, “placeholders” and “hooks” have been used when names of parties or business services. For future commercial or production grade use of these Rules, implementers would replace the example parties, service descriptions, etc, with the respective applicable names or terms.

   These System Rules are tailored to be directly usable and adoptable by existing personal data stores companies but also to adaptively scale in support of emerging big data marketplaces and personal data ecosystems. The increasing value, volume, velocity and variety of transactions flowing web-based applications today is straining the current models and architecture to the breaking point. While the technology exists to push bandwidth and meter usage in various ways, current business and legal foundations are inadequate to establish trustworthy interoperability and predictable legal outcomes for desired big data services and transactions. This draft provides a novel approach to address these needs, with a mix of standard reusable rules and agreements and a set of modular, extensible and interoperable individual rules and components.

   Personal data, as an asset class, will exist in networks, systems, markets, stores, services and transaction types that are at once very secure and very open, simultaneously high velocity and high volume, and both dynamically evolving and reliably predictable. The business models and relationships defining the scope and substance of transactions and services require a much more robust yet simple to apply set of legal and technical tools to adaptively design and deliver deals and lines of business. The legal agreements reflecting granular grants of authorization and governing vast numbers of globally distributed parties requires service oriented systems of rules and a data-driven contract infrastructure connecting all parties. The demands to rapidly deploy new architectures and services, maintain high levels of performance and reliability while also ensuring tight and responsive security, oversight, controls and response measures across the network, systems, applications, data and extended enterprise demands modularity, interoperability and resilience of technology that is all but unprecedented. However, there are today small pockets of best practices and exemplars of personal data and individual federated identity. These early instances provided the design patterns underying the Model System Rules.

   A key concept underlying these Model Rules is that the rules and corresponding agreements exist within a broader context and apply to parties that frequently also have existing commercial relationships and business arrangements. The Rules anticipate and support this fact through the “Trust Stack” approach, which anticipates the Rules being “layered” on top of existing business or other “trusted relationships” but not conflicting with or replacing the existing commercial contracts and other arrangements of the parties. This is fundamental to the design and intended use of the Model Rules and is a key way this approach can ensure true interoperability at the business and legal levels while being adoptable for a wide variety of different business models and commercial or other relationships. That Model Rules deliberately stop short of assuming, much less insisting upon, presumed business models or methods, posited legal rights or responsibilities, or particular technical services or standards.

   The way this plays out in the instance of these Model Rules for Personal Data Store Account Holders and Service Providers is two-fold. First, it is expected that the Third Party Service Providers will have an independent “Terms of Service” with any “Individual User” of the Personal Data System and that the “Terms of Authorization” are supplemental to those underlying business contracts. Second, it is similarly assumed that the System Provider will have deeper and more complex and broadly scoped business contracts with Third Party Service Providers, such as the “Developer Agreements” or “API Access Terms” or other commercial app market access terms. Therefore, the “Participation Agreement” between the System Provider and the Third Party Service Provider is designed to layer on top of that contract and not to conflict with or replace it. The specific terms that are common to the standardized, modular and scalable Model Rules are focused on the subset of issues and common needs for cross-boundary secure data sharing and not focused on the highly idiosyncratic commercial fee structures, service levels and other business model related aspects of a given implementation. In this way, the Model Rules can be used by a variety of different businesses and in many contexts and still allow many parties to have confidence that certain key issues are clearly addressed by any other parties that use and apply the Model Rules. [↑](#endnote-ref-1)
2. The Model Rules, while deliberately avoiding presumed particular business models and choices about the nature, scope and substance of relationships, services and functionality, do nevertheless follow certain conventions and are keyed broadly to the use of distributed data sharing and identity federation. The business, legal and technical rules in part address the same topics from their respective viewpoints (eg requirements related to the provision and use of a service, specification of roles and relationships, etc) and in part address topics that are unique to their individual domain. The underlying Model Rules from which this document is derived provide a highly modular “plug-and-play” set of re-usable and extensible rules as well as methods for defining and applying sets of Rules appropriate for a given scenario of use. By way of example, the MITRE Corporation External Identity Federation Trust Framework System Rules demonstrate how the Model Rules can be applied to the scenario of corporate IT extended enterprise identity services supporting employee, contractor and trusted partner “single sign-on”. The intended scope and purposes for this common business-to-business scenario and associated use cases results in partly different business rules such as the scope and functions to be provided and the legal relationships and expectations as well as various aspects of the technical and security implementation choices and requirements. Conversely, there are several very generic facets of systems using the Model Rules as a basis for developing System Rules that are common, re-usable and can significantly simplify and accelerate adoption of next generation data and identity solutions, as well as enable and accelerate interoperability with a vast array of external systems, services and applications.

   This document demonstrates how the Model Rules can be applied to a postulated and generalized business offering personal data and individual identity services commercially to individual consumers. These Personal Data and Individual Identity System Rules also reflect the current common practice of enabling consumers with accounts on a personal data service to grant authorization for access to their data to external third party service or application providers. Examples of this use case include a social network site, photo sharing site or document collaboration site that provides it’s users the capability to sync or otherwise integrate their data on that site with a service provided by another company, such as Dropbox, Google Apps, Facebook or Evernote. [↑](#endnote-ref-2)
3. Within this document, some content is explicitly intended as illustrative examples of potential ways the current research program could be rolled out in commercial or other production offerings, such as the particular types of data services and the specific work flow and interchange specifications between interoperating parties. Placeholder business capabilities, legal relationships and technical functions serve as examples of the ways these integrated systems can be configured and how parties can structure and represent those implementations within the construct of these model system rules and agreements. Placeholder content is identified and discussed in this supplemental guidance and commentary addenda. [↑](#endnote-ref-3)
4. The hooks are designated by words or phrases within [brackets] and that are presented in their intended final form, requiring only insertion of the specific identifiers or other names or information indicated, such as the legal name of a party or the URI or URL of a defined online resource such as, for example, a policy document or the interface for a directory entry or other database record. [↑](#endnote-ref-4)
5. As applied to multiparty consortia or systems of systems, these System Rules would include many sets of terms not present to cover the postulated use case of a single company providing a PDS. To the extent multiple PDS and affiliated analytics or other personal data related service companies banded for the purpose of joining a network with high regard for and protections of personal control and superior capabilities for interoperability and scaling, these Rules could easily be adapted to their case. Among other things, more terms in all three sections would be required, potentially including in the business section new provision for such functions as:

   1.6 Operational and Financial Practices

   1.6.1 Points of Contact

   1.6.2 Invoicing and Billing

   1.6.3 Support Coordination and Escalation

   1.6.4 Business Continuity and Change Management [↑](#endnote-ref-5)
6. The business scope and intended scenarios of use have been somewhat generalized to provide a flavor and example how these System Rules can be applied to personal data stores and services generally. The clinical and other user testing and research on the DARPA project will not require a sophisticated set of rules. However, if a system such as this were to be applied in the narrower context, it might read something like the: “The System Rules warfighters returning from deployments. These include contractual governance and enforcement through binding legal agreements, anonymized IDs that cannot be traced back to device IDs, user selection of sharing levels, privacy technologies for anonymized aggregation, use of secure OAuth tokens for separation of authentication from service delivery, and encrypted storage of sensitive data.”

   In larger scale and more complex systems, it may be necessary to literally agree upon a set of Use Cases that are more detailed that the general intended scenario and which can serve as a tool to help the governing body membership identity the actual requirements and constraints applicable or desirable for the System. The substance and scope of the System as well as the requirements and rules for the parties can be detailed based on the general contours and content of the scenario. The method used to develop accurate and aligned business, legal and technical System Rules involves eliciting the business roles, functions, flows, roles, relationships, legal parties, transactions, rights, responsibilities, technical actors, actions, interactions, standards, security and other relevant input from the appropriate executives or other staff at the organization (or organizations) deploying a personal data system results in a more complete and adoption-ready launch and operation. For purposes of this draft set of System Rules, the business, legal and technical context and usage is based upon composites of existing common approaches and practice in general use and uses the MIT DCAPS “OpenPDS” software, visual analysis service and other features as key reference points. [↑](#endnote-ref-6)
7. The System Architecture would include, in addition to an extended enterprise service oriented type of architecture also the applicable technical use cases describing the actors and actions envisioned and enabled by the System and System Rules. The types of architectural aspects of the System this sections would describe or reference may well include: System Thresholds; Personal Data Store; PDS Services and Components; Third Party Services and Apps and potentially any Marketplace for apps or other services and transactional details. [↑](#endnote-ref-7)
8. When applied to multiple PDS providers, this section would include a required minimum set of “Core Services” to be provided by any PDS operator within the System and an optional set of “Extended Services” that have been approved for provision within the System and are supported with some level of shared infrastructural shared services including Core Legal Event Registry services and enterprise bus routing and optimization services. This approach allows a more sophisticated and flexible result whereby services that are not approved but are not prohibited under the Rules due to violation of a business legal or technical requirement may also be offered by PDS providers but would not be listed in this section or supported by the Rules or the System. [↑](#endnote-ref-8)
9. See the Addenda titled “Approved Scopes and Grant Types” for more information on the approach to this topic and how it is intended to provide a basis for integration of the contractual and technical code so as to ensure the privacy and control of Principal Users and the predicted legal results expected by all Parties. [↑](#endnote-ref-9)
10. Security envisioned for commercial offering and production grade operations of the System has been benchmarked, by permission of, the best practices of premier personal data store provider Personal.com. [↑](#endnote-ref-10)