FLORIDA COURTS TECHNOLOGY STANDARDS
SECTION VII: DATA EXCHANGE
[ALL-IN-ONE DOCUMENT]

{11/1/2020}

E: TextBookDiscrimination@gmail.com
W: www.TextBookDiscrimination.com

visit TBD's website for the most up-to-date information

TABLE OF CONTENTS | SECTION 7: DATA EXCHANGE

#	Section	Title	Page
G01	7.1.0	Introduction	4
G02	7.2.0	Governance	6
G03	7.3.0	Data Exchange Security	7
G04	7.4.0	Transport	9
G05	7.5.0	Transfer Framework	11
G06	7.6.0	Integration Toolkit	13
G07	7.7.0	Conformance	14

-	n/a	Appendix	15

FLORIDA COURTS TECHNOLOGY STANDARDS

SECTION: 7

CAPTION: DATA EXCHANGE

ITEMS: 7.1.0 through 7.7.0

ITEM 7.1.0 | INTRODUCTION

The exchange of court data represents an extremely dynamic challenge for all involved. The demands of efficiency, timeliness, accuracy, and confidentiality combine to impose significant, often conflicting, demands on the exchange process. Traditionally, these challenges have been met locally with solutions targeted to the specific court data management system involved. However, if the court system is to keep pace with the evolving information age, a more global solution is required. The task of this specification is to define a sufficiently rigorous mechanism to standardize the transfer of data between two or more data systems while remaining flexible enough to tailor the exchange particulars required to the specific needs of those systems.

For purposes of this standard, interaction is being considered between the following entities:

- Clerks of court case maintenance systems and supporting systems (referred to as clerk CMS).
- Circuit court judicial viewer and/or Court Application Processing Systems (referred to as CAPS).
- State-level Judicial Data Management Services system (referred to as JDMS)

The decentralized nature of the relationships between county and circuit, circuit and state and county and state, and the variety of data management solutions deployed guarantees that the transfer of data between various entities within and outside of the court system is a complex matter. Multiple counties may maintain individual CMS's or may share the same CMS. Similarly, circuits may share a single CAPS among multiple counties within their jurisdiction or deploy individual CAPS as appropriate. Consequently, this standard must define a data transfer mechanism that satisfies the need to exchange data efficiently and effectively between court partners and that is independent of the complex relationships mentioned above while simultaneously guaranteeing the highest levels of security, resilience, and privacy of the data contained and shared among these systems.

However, it is not possible to compose a standard describing a limitless set of possible interactions. The intent of this standard is to define the mechanism by which a data transfer event is initiated and completed and to provide a description of the data package that is exchanged. It is not concerned with what must

happen to a particular piece of data once it is received. Those details are left to the consuming system.

This Data Exchange Standard incorporates other existing, non-proprietary standards and specifications wherever possible. In particular, this standard has dependencies on the [ECF] (See Appendix A), [NIEM] (See Appendix A), [FIPS-180-2] (See Appendix B), and the World Wide Web Consortium (W3C) (See Appendix A). The terminology used in this standard to describe the components of the Data Exchange architecture conforms to a Service Oriented Architecture (SOA) (See Appendix B and C).

ITEM 7.2.0 | GOVERNANCE

Once the standard is approved, the Data Exchange Workgroup will schedule quarterly conference calls with at least one meeting in-person annually.

Changes to these standards must be approved by the **Florida Courts Technology Commission** ("**FCTC**") based on recommendations of the Data Exchange Workgroup before implementation. Requests for changes to these standards will be submitted to the Data Exchange Workgroup via the Office of the State Courts Administrator ("OSCA") and reviewed at the next scheduled meeting and a recommendation will be made to the **FCTC.**

Volusia County completed a pilot project testing the data exchanges. The documentation can be accessed at http://app02.clerk.org/menu/ccis/.

Nonconformance to these standards, once adopted, may be referred to the **FCTC.**

ITEM 7.3.0 | DATA EXCHANGE SECURITY

As noted in the Introduction section, version 1.0 of these standards will cover the exchange of data between local CMS, CAPS, and state-level JDMS systems and may include interactions with other state-level systems such as the Comprehensive Case Information System ("CCIS") as appropriate. Subsequent versions of this standard may expand upon and include data exchange between additional systems or stakeholders.

The Data Security Model should contain the following elements:

- Data Storage Encryption: All data stored electronically in locations other than those where the systems are located must also be encrypted, (e.g., an offsite backup facility). This also applies to any data extracted from the CMS with the intention of performing bulk transfers into other systems.

- Workstation Security: All end-user workstations or devices must maintain an up-to-date, industry-standard anti-malware system to protect the information being consumed by the end-user. This may be exempted only in the event that a business case has been developed showing that the end device cannot be kept current. In this event, the organization providing the data must be notified before the exchange.

- Mobile devices: No data may reside in mobile devices beyond the current session. If such a device is deployed or used for the "consumption" of information, a VPN solution must be deployed and managed by the courts.

- Cleaning Hard Disks: If at any moment a portable Hard Disk Drive or similar technology is used to transfer data among systems, the storage device must be sanitized using the DoD 5220.22-M approach.

- Firewalls: Firewalls are required when data must transport through an external network to reach its destination. This will be through a firewall specific source and destination (IP and port) defined in the firewall to prevent unintentional access to source/destination servers.

- User Credentials: When credentials (passwords) are necessary to access or transmit data among systems, the password should be a complex (upper, lower, numeric, and special character) combination password no shorter than 8

characters and renewable every 90 days. Provisions should be taken to deny the reuse of the previous 5 passwords.

• Security Updates: To mitigate vulnerabilities at the host and PC level, systems must have security updates applied frequently (preferably via automatic update); checks to ensure any system is not vulnerable should be performed before bringing it into production.

ITEM 7.4.0 | TRANSPORT

All data transport should be secured and encrypted in compliance with ECF 4.0.1, Section 5, Service Interaction Profiles, as augmented below. See Appendix B – [FIPS-180-2] and Appendix C).

- Data Exchange Protocol: Enhanced transport requirements shall be Secure HTTP (HTTPS) that consists of the standard HyperText Transfer Protocol (HTTP) layered on top of a secure Transport Level Security (TLS) session. To maximize security, any public-facing interface should be registered with a Certificate Authority ("CA); either a commercial service or maintained via the State Courts System. For the best security, 2048-bit (or more) key lengths should be used. For closed data center environments where communications occur between trusted servers, TCP may also be used (See Appendix A).

- Web Services: To ease implementation, the use of the Web Services Description Language ("WSDL") is strongly recommended, as it helps automate the creation of compliant interfaces for clients by providing a machine-readable description of the web service.

Data transport includes the transfer of data to the state and other repositories. For example, Section 2, E-Filing Standards, identifies the capability to transfer case and court activity data, both as single records and in bulk, to state-level data repositories as an essential capability of court data management systems. Transfers may be made for a wide variety of purposes including routine activity reporting, program and performance monitoring, resource allocation, court operations management, and data warehousing. The transfers may use a wide variety of data exchange scenarios, e.g., a data transfer initiated by a local data provider to a receiving state repository in response to changes within the underlying data being reported (event-push), or a transfer where the request originates from the repository to the local data management system (timed-pull). Consequently, the general web services capability established at either end of the data transfer should be capable of handling both types of transactions. The specific strategy, event-push or timed-pull, should be identified by the entity originating the transaction as part of the data request package definition.

It is recommended that data transfer occur using the lowest level, stable technology suitable for the task, in conformance to this standards document. However, it may be necessary to define

alternate data transfer mechanisms, such as FTP or FTPS, in order to maintain compatibility with legacy reporting systems or when reporting is sufficiently short-term or is of such a nature as to not justify the cost to develop a web services solution. The suitability of alternative transfer mechanisms should be determined by the entity originating the reporting requirement and approved by this standard's governing body.

While this data transfer standard is comprehensive, not all elements defined for a data request package may apply to a given exchange scenario. Since the data request may involve a large number of agencies, the entity originating the request should define a data transfer package description document detailing the format and content of the data being transferred and identifying the appropriate auditing and tracking elements as provided in this standard. This information may be included as part of the integration kit discussed below. If necessary, to ensure data transfer integrity, the service enabling the specific data transfer should provide for immediate, synchronous response to, for example, allow a service to initiate a transfer and the receiving service to signal success or failure of a transfer. (See Appendix C).

ITEM 7.5.0 | TRANSFER FRAMEWORK

The court system is adopting an enterprise standard for data management. Conformance to this standard requires the use of an SOA as the foundation for all data transfer. This approach views data exchange, not as a series of isolated data projects with each exchange subject to separate and unconnected rules. It is expected that data exchange projects can be built from a set of reusable modular components that can be mixed and matched as needed to provide the necessary functionality. The data exchange mechanism defined in this standard can serve as an architecture for data transfer in that the mechanism is capable of exchanging data between two endpoints.

The data transfer can be broken down into three types of information:

- Metadata describing the data being transferred.
- Sufficient tracking and auditing information to ensure reliable transmission, receipt, and messaging.
- The actual data to be transferred.

The integration toolkit discussed below will contain sufficient information to describe the data exchange. While some of the data needs can vary widely between jurisdictions, there are many types of common data exchanged, across all entities within the state. As specific data exchanges are defined, and appropriate integration kits are built, it is planned that these standards will be expanded with a library of namespaces, XML Schemas, Major Design Elements (MDEs), and data dictionaries for common data exchanges (See Appendix C). This library will further help standardize data exchange within the court system and simplify the implementation of new exchanges across the state. Data Exchange Content Models will be developed to facilitate this standardization (See Appendix C and D.) In the context of web services, Major Design Elements (MDEs) is the conceptual representation of the exchange (See Appendix C) exposing a canonical set of core capabilities (See Appendix F). The Data Exchange architecture is divided into two principal elements:

- Core specifications that define the MIDEs and the operations and messages that are exchanged between the MDEs.
- Service Interaction Profiles (See Appendix C) are specifications that describe the communication

infrastructures that deliver the messages between MDEs. Any Data Exchange MDEs will follow these two principal elements as formulated in the ECF 4.0.1 (or current) standard for data exchange. In addition, the data transfer framework components of:

1. Meta description.

2. Audit and tracking information.

3. Data content is to be constrained through the use of namespaces and XML Schema Definition ("XSD") files.

Multiple namespaces can be included in one or more XML Schema Definition files that include all necessary constraints that are specific to the particular data transfer. The Data Exchange XML schemas are implementations of the data exchange content models (See Appendix C and D). They are the only normative representations of the messages.

ITEM 7.6.0 | INTEGRATION TOOLKIT

An integration toolkit should be provided for any implementation purposes. This toolkit consists of detailed documentation identifying:

- A plain language name for the integration toolkit.
- A Universally Unique Identifier (UUID) for the integration toolkit (mandatory element) – A UUID for the integration toolkit as agreed upon by the entities involved.
- A UUID for other existing or new data exchange specifications – This UUID allows versioning of the specification and promotes controlled upgrades and modifications between different data systems.
- A clear plain language description of the contents of the data being transferred including appropriate references to specifications if necessary.
- Example XML requests and responses, data dictionary (including the detailed description/format of each data element or attribute), references to appropriate business rules, relevant standards and definitions, XML schema definition files, theory of operation, Major Design Elements – (MDEs, and sample usage cases for each MDE (See Appendix C).

ITEM 7.7.0 | CONFORMANCE

Conformance to this standard does not apply to existing systems that are technically incapable, or it is cost-prohibitive to conforming to this standard and data exchanges.

APPENDIX

COPYRIGHT NOTICE

ORIGINAL SOURCE

#	Item	Link
1	Original Source	www.FLCourts.org

CONTACT INFORMATION

E: TextBookDiscrimination@gmail.com
W: www.TextBookDiscrimination.com

Congratulations! You're now ***booked up*** on Section VII (*Data Exchange*) of the Florida Courts Technology Standards!