MEMO

FR: **Joe Ferrada, Family Center of Washington County**
TO: **House Energy and Technology Committee**
DA: **Feb. 18, 2022**
RE: **ADDITIONAL TECHNICAL INFORMATION ON PROPOSED CIS COMMUNITY DATA SYSTEM**

Background

The CIS Community Data System was initially established as a single instance developed for the Family Center of Washington County (FCWC). The system has been in use for the last five years and conforms with the state CIS data reporting requirements.

Over the years we have worked with CIS staff to make sure the system is updated when requirements change. The goal of the expansion proposal is for the system to eventually integrate with the state CDDIS/CCWIS system, subject to interest and approval of all parties involved. To that end we are committed to working with DCF and ADS to align the FCWC system for possible future transition and integration.

ECM and Salesforce Security Overview

The combination of ECM + Salesforce Security and Sharing features enables the FCWC system to keep data secure and control data access and at the same time implement flexible data sharing rules. ECM + Salesforce roles, profiles, permission sets, public groups, and criteria-based sharing features support many different types of sharing models.

1. Salesforce security is built from the ground up. Salesforce provides us with innovative tools and educational resources necessary to protect our data.
2. Health Check is a free tool that comes standard with Salesforce products. Built on the system's core platform, it allows admins to manage our organization's most important security settings in a single dashboard. Using Health Check, admins can seamlessly identify and fix potentially vulnerable security settings with one click. Customers can also create custom baseline standards to align closer with the individual security needs of their business.
3. Login IP Ranges limit unauthorized access by requiring users to login to Salesforce from designated IP addresses. By using Login IP Ranges, admins can define a range of permitted IP addresses to control access to Salesforce. Those who try to login to Salesforce from outside the designated IP addresses will not be granted access.
4. Multi-factor authentication (or MFA) adds an extra layer of protection against common threats like phishing attacks, credential stuffing, and account takeovers. Salesforce requires customers to enable MFA in order to access Salesforce products.
5. As part of our overall security strategy, Salesforce Shield additional security is available. While Salesforce is equipped with many out-of-the-box security controls, Shield complements existing security features with enhanced encryption, app and data monitoring, and security policy automation. Shield can help admins and developers build a new level of trust and transparency in business-critical apps.
6. A custom domain name helps FCWC manage login and authentication for our organization in several ways:
   - Block or redirect page requests that don't use the new domain name
   - Set custom login policy to determine how users are authenticated

    - Work in multiple Salesforce organizations at the same time
    - Let users log in using a social account, like Google and Facebook, from the login page
    - Allow users to log in once to access external services
    - Highlight business identity with unique domain URL
    - Brand login screen and customize right-frame content

7. Users sometimes leave their computers unattended, or they don't log off. The system can protect the application against unauthorized access by automatically closing sessions when there is no session activity for a period of time.
8. Salesforce requires all secure org connections to use TLS 1.2 or higher to ensure the most secure environment and continued payment card industry compliance.

Data governance

As part of the proposed expansion, FCWC will establish a set of policies and procedures that ensure the quality, accuracy, and usability of data. These will also be critical for ensuring ethical use, protecting privacy, and confidentiality.

Participating members will be required to sign an agreement delineating the terms of membership. The agreement would include:

1. Establishing policies and processes for data governance at all stages of membership
2. Protecting privacy of clients
3. Establishing and complying with a data security plan

Policies and procedures for managing the data system would include defining clear lines of authority in each organization with respect to roles for data protection and accountability in line with current CIS contract language.

A Community Data System Governance Committee would be established. The Committee would include representation from designees of organizations who are active participants in the CIS Community Data System, state agency representation, as well as the data system administrator. The Committee should be formalized with an agreement that defines the mission, goals for data governance.

The Committee members drive the agenda for the Community Data System such as decision-making process for changes and upgrades to bring into the system, which policy or program questions are most urgent to discuss, access, security, tech support, expenses, etc.

Security

Protecting privacy and human subjects involves protecting data with personally identifiable information (PII) or protected health information (PHI under the Health Insurance Portability and Accountability Act, or HIPAA) and ensuring compliance with the terms of the data agreements and local, state, and national privacy laws that govern access and use of data.

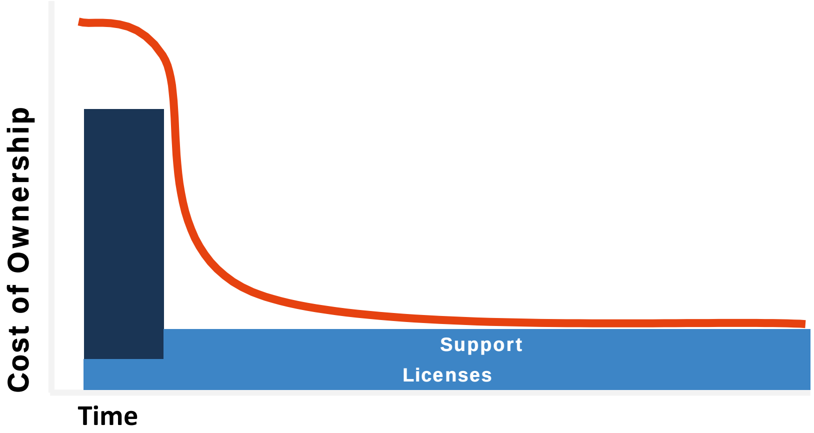
Establishing data security is a prerequisite to acquiring confidential data and must be maintained to protect against misuse and unauthorized data breaches. The data security plan defines who has access to data, how data will be held confidential and secured during transfer and storage, how vulnerability to attacks will be assessed, and what protocols are established in the event of data misuse or breach, and to monitor compliance and train staff.

Why do we need an expanded CIS data management system now?

- Providers will have more time to work with clients, rather than all the hours they now spend on paperwork – every hour saved through efficiency means another hour available to help children and support families.
- Families won't have to repeat their stories over and over again with every provider – shared files save time and lessen trauma for families, as they don't have to relive their challenges multiple times.
- Children and families will receive higher quality, more targeted services when they are served by CIS professionals whose work is more fully informed by data that allows them to analyze what works and what doesn't, and how to best direct their limited resources
- Organizations will be able to report out real time data to the state and legislators without spending excessive periods of time aggregating paper and excel data from multiple organizations in each region and across the state

What about ongoing costs?

While ongoing costs will exist, the vast majority of the costs associated with this expansion will be in the set-up, training, and implementation stage – all of which are covered by this proposal. Ongoing costs would be minimized to the extent that the CIS data system was incorporated into larger systems at CDD, since licensing, training, and technical support costs would be spread over more users and programs.



Exponent Case Management

- ECM's configuration engine means clients can easily modify existing programs or stand up entirely new programs on their own.
- New features are continually being paid by Exponent and the ECM community, developed, and pushed to your Salesforce instance.
- The yearly user license fees pay for continuous upgrades, security enhancements, and maintenance. The fees are absorbed by each CIS community partner as part of their ongoing overhead costs.