Community-Based Care Information System Requirements

The department maintains information in the Florida Safe Families Network (FSFN) Information System (Comprehensive Child Welfare Information System (CCWIS) for the child welfare system for the state of Florida. The department also maintains access to the Vital Statistics system to identify and verify data for children and parents when information regarding names, dates of birth, the place of birth or other pertinent addresses is received from the abuse hotline or other lawful sources. The provider must enter data into, and retrieve data from, these applicable systems. In accordance with Florida Statutes, Florida Administrative Code and departmental standards and procedures, the provider shall be required to exercise due diligence to ensure and maintain the accuracy, timeliness, and appropriate levels of security of information entered into, or retrieved from, these systems. It is expressly understood that the provider's violation of Ch. 119, F.S. or any associated Florida Administrative Code and departmental standards and procedures, may constitute sufficient grounds for a determination that the contract has been breached.

A. Security

1. The provider shall comply with all applicable laws and procedures pertaining to security and confidentiality including, but not limited to, those listed in the Community-Based Care Authority and Requirements Reference Guide.
2. The provider's own systems and premises shall be subject to inspection by the department's representatives at any time to verify compliance with security requirements.
3. Any data communications involving the department may also be monitored by department security or systems personnel for compliance with these requirements or misuse of the systems.
4. In the event that the provider is allowed to electronically connect to any of the department's facilities, the department may suspend or revoke that connection at any time without notice if the department has reason to believe that the security of the department's systems may be compromised by a continuation of that connection.
5. In the event the provider purchases, develops or maintains its own electronic information systems to support services provided through this contract, the department must have access to all information necessary to audit and examine such information in its native format, using access devices (terminals, personal computers, or other devices required) made available for this purpose by the provider. The provider must provide the department's representatives with the necessary system user accounts and passwords to access all information related to this contract which may be stored in the provider's systems. All Covered Data must be encrypted in transit and while at rest.
6. The department may require the provider to accurately complete a self-audit questionnaire relating to the electronic information systems the provider and any subcontractors or affiliates participating under this contract use.
7. Material security violations or improper information disclosures shall constitute sufficient grounds for a determination that the contract has been breached.
8. At least quarterly, the provider will provide a listing to the department that includes, at a minimum, the name and user IDs of all users with access to above systems. Within 10 days of receipt of this listing, the department must certify to the provider Contract Manager that all user IDs listed are currently active and necessary. Any provider user IDs are to be defined as to whom they are for and the reason for the access. During the term of the contract, the provider must also notify the CBC's FSFN Security Officer when any staff with access to mentioned systems is no

longer employed for any reason. This notification must be provided within 1 business day of the separation.

9. The following summary of key security standards are applicable to all data covered by federal or state laws or regulations (Covered Data). The following list is not intended to be, and is not, exhaustive. The provider must comply with all security requirements related to Covered Data and any other State of Florida data provided to, or collected by, the provider acting on behalf of the department as its contractor. Further, the provider's employees, subcontractors, agents, or other affiliated third-party persons or entities, as well as contracted third parties, must meet the same requirements of the provider under this contract and all agreements with the provider's employees, subcontractors, agents, contractors or other affiliated persons or entities shall incorporate the terms and conditions of data security into any contractual relationships established. The Department reserves the right to review these agreements to ensure the security standards are included:

a. Access Controls:

1) Viewing and modification of Covered Data must be restricted to authorized individuals as needed for business related use according to the principles of least privilege and minimum necessary. Controls will ensure that legitimate users cannot access stored software or system control data without authorization.
2) Unique authorization is required for each person permitted access to Covered Data and access must be properly authenticated and recorded for audit purposes, including HIPAA audit requirements.
    - The provider must ensure that all employees or contractors receive a Data Security packet.
    - Before an employee or contractor can receive system access, Data Security must receive an Access Authorization Request Form (Attachment A) signed by the employee or contractor and their supervisor requesting a user code. The form should identify system access needed for their assigned group, unit or section. In addition, the employee or contractor must attach a copy of their most current Security Awareness Training certificate and any additional required system access forms.
    - The previous supervisor of a reassigned employee or contractor must review all work products the reassigned employee has created to determine what should be retained, moved, or deleted, and then take the appropriate action.
    - Within five (5) days of the employee or contractor’s reassignment, the previous supervisor must notify Data Security to revoke or suspend the reassigned employee or contractor’s access rights.
    - If an employee or contractor is not reassigned but has a change in job duties, the supervisor must notify Data Security of the change in duties within five (5) days to ensure access privileges are appropriate for their job responsibility.
    - Before Data Security can grant access to the data and systems necessary to perform a worker’s new job assignment, Data Security must receive a completed Access Authorization Request Form (Attachment A), which is signed by the employee or the contractor and their supervisor.
    - The last supervisor of a terminated employee or contractor must review all work products created with the terminated worker’s user code and/or access code to determine what should be retained, moved, or deleted and upon completion must notify Data Security to revoke all access authorization of the terminated employee

or contractor. The supervisor shall take appropriate actions to ensure the DCF Office of Information Technology Services has the capability to access all pertinent data created by the terminated workers. This applies to mainframe, servers, and personal computers.

- When necessary, the appropriate manager may request emergency removal of user access and then follow up with the normal procedure.
- Supervisors will conduct and document quarterly reviews of staff access privileges.

3) Access to all Covered Data provided to the provider's employees, subcontractors, contractors, agents, or other affiliated persons or entities must meet the same requirements of the provider under this contract and all agreements with same shall incorporate the terms and conditions of data security in the access authorization.

b. Copying/Printing (applies to both paper and electronic forms):
   1) Covered Data should only be printed when there is a legitimate need.
   2) Copies must be limited to individuals authorized to access the Covered Data and have a signed CF0114 on file with the department.
   3) Covered Data must not be left unattended. 4) Covered Data must be properly destroyed.

c. Network Security:
   1) All electronic communication including, but not limited to, Covered Data between the provider and the department shall use data encryption or a Virtual Private Network connection to ensure a secure file transfer at no additional cost to the department.
   2) Covered Data must be protected with a network firewall using “default deny” ruleset required.
   3) Servers hosting the Covered Data cannot be visible to the Internet, or to unprotected subnets.

d. Physical Security (Servers, laptops and remote devices on which Covered Data is stored) (For purposes of these standards, mobile devices must be interpreted broadly to incorporate current and future devices which may contain or collect Covered Data.):
   1) The computing device must:
      - Be password-protected using a complex password that meets State complexity requirements as defined in Rule 71A-1.002(21) Locked or logged out when unattended.
      - Secured using a password-protected screensaver with the automatic activation feature set at no more than 15 minutes.
   2) Servers must be hosted in a secure data center hardened according to relevant security standards, industry best practices and department security policies.
   3) Physical access to servers containing Covered Data must ensure physical access is monitored, logged and limited to authorized individuals 24/7.
   4) Routine backup of Covered Data is required and backed up Covered Data must be stored in a secure off-site location.

e. Remote access to systems hosting Covered Data:
   1) Remote access to Covered Data must be restricted to the local network or a secure virtual private network.
   2) Unsupervised remote access to Covered Data by third parties is not allowed.

3) Access to Covered Data by all third parties must meet the same requirements of the provider under this contract and all agreements with same shall incorporate the terms and conditions of data security in the remote access authorization.

f. Data Storage:
   1) Storage of Covered Data on a secure server in a secure data center according to relevant security standards, industry best practices and department security policies is required.
   2) Covered Data stored on individual workstations or mobile devices must use whole disk encryption and a password that meets State password complexity requirements as defined in Rule 71A-1.002(21). Encryption of backup media is similarly required to be encrypted.
   3) Covered Data is not to be transmitted unless encrypted and secured with a digital signature.
   4) Covered Data must be stored in an encrypted state at rest.

10. The provider must meet all of the department and State requirements for individual employee security, information security, and physical security of all non-public data in the possession of the provider.
11. The provider acknowledges that all Covered Data, other data and department content uploaded to the provider's servers, workstations or mobile devices from the department, or made accessible to the provider's servers, workstations or mobile devices or personnel remains the property of the department.
12. Determination provisions related to Data:
    Within 30 days after the termination or expiration of this contract for any reason, the provider shall either: return or physically or electronically destroy, as applicable, all Covered Data provided to the provider by the department, including all Covered Data provided to the provider's employees, subcontractors, agents, or other affiliated persons or entities according to the standards enumerated in D.O.D. 5015.2; or in the event that returning or destroying the Covered Data is not feasible, provide notification of the conditions that make return or destruction not feasible, in which case, the provider must continue to protect all Covered Data that it retains and agree to limit further uses and disclosures of such Covered Data to those purposes that make the return or destruction not feasible as the provider maintains such Covered Data. This includes any and all copies of the data such as backup copies created at any provider site. Upon request by the department, made before or within sixty (60) days after the effective date of termination, the provider will make available to the department for a complete and secure (i.e. encrypted and appropriated authenticated) download file of department Covered Data in XML format including all schema and transformation definitions and/or delimited text files with documented, detailed schema definitions along with attachments in their native format. The downloaded file shall include all Covered Data provided to the provider's employees, subcontractors, agents, or other affiliated persons or entities must also comply with this requirement. The provider's employees, subcontractors, agents, or other affiliated persons or entities must be available throughout this period to answer questions about data schema, transformations, and other elements required to fully understand and utilize the department's data file.

B. Liability for System Failure

1. The department is not liable to the provider for a failure of any of the department's systems or for the degradation or disruption of any connection or system. Provider loss or diminution of access

to the department's systems for any reason shall not excuse the provider from its obligations under this contract.

2. The provider shall be held accountable for late data input due to a department systems failure of less than one working day. Department systems failure of more than one working day shall be calculated as follows: For each additional working day of department systems failure, the provider shall have two working days for data input before they are held accountable for late data input.

C. Vital Statistics

1. The Vital Statistics Birth Registration System maintains official records of births within the state, as well as births to Florida residents which occur out of state. Authorized users have on-line access to birth records to identify and verify data for children and parents when information regarding names, dates of birth, place of birth or addresses is received from the abuse hotline or other lawful sources.
2. The provider shall comply with the current Memorandum of Understanding (MOU) between the department and the Department of Health (DOH), which sets the parameters for access to the Vital Statistics system by the Family Safety Program and its agents.

D. Florida Safe Families Network (FSFN) Requirements

Florida Safe Families Network is the department's system of record for all child welfare casework and is administered under federal Comprehensive Child Welfare Information System (CCWIS) regulations. The Comprehensive Child Welfare Information System (CCWIS) regulations and governs the way in which state and tribal title IV-E agencies will claim federal funding for child welfare information systems that support the administration of title IV-E and IV-B programs. The CCWIS regulation includes new requirements around design, data quality, and data exchange standards, and aligns with current and emerging technology. The provider specifically agrees that Florida Safe Families Network will always contain the most current and the most accurate information regardless of any other systems employed by the provider.

1. The provider shall collect, enter and maintain all data to meet Florida Safe Families Network system's requirements in accordance with federal requirements and department policies and procedures, including timeliness criteria. This requirement is that FSFN is to be updated within 2 business days after a service event occurs.
2. The provider shall participate in CCWIS Data Quality Plan definition, monitoring, and improvement initiatives.
3. Caseworkers shall be responsible for verifying on a regular basis, and no less than monthly, the accuracy, completeness, and timeliness of all data relating to their assigned cases within Florida Safe Families Network.
4. The provider is responsible for purification of data for the geographic area served by the provider in State systems that may be necessary before any future automated conversion of data from current systems to Florida Safe Families Network.
    a. This includes data entered before the provider assumed responsibility for services.
    b. The provider is also responsible for any manual data conversion activities required.
    c. If additional funds are made available to the Region for this purpose, a proportionate amount may be added to this contract for a similar level of effort.

5. Joint Application Development (JAD) Sessions and User Acceptance Testing;
    a. The provider shall participate in JAD sessions and user acceptance testing during the development and operation of Florida Safe Families Network.
    b. The provider shall be responsible for any travel costs associated with attendance at these sessions.
6. Application Training.
    a. The provider shall participate in application training for use of Florida Safe Families Network as required during the deployment of future Florida Safe Families Network functionality.
    b. The provider shall be responsible for any travel costs associated with attendance at these training sessions.
7. Site Survey.
    a. The provider agrees to allow the department to conduct a site survey to determine needs related to the implementation of Florida Safe Families Network at the provider's site(s).
8. Equipment.
    a. The provider shall not use equipment provided by the department and purchased with Florida Safe Families Network system's funds for any purpose other than to support staff providing Title IV-E and IV-B eligible services in accordance with the department's federally approved cost allocation plan for Florida Safe Families Network.
    b. Florida Safe Families Network computer equipment shall not be transferred, replaced or disposed of by the provider without prior permission of the department's contract manager.
9. The provider shall not have access to State owned applications, e.g., FSFN, ICWSIS, etc., to resolve data issues requiring direct database access, make software changes, add programming, etc. The provider shall be responsible for, with appropriate access authorization to the State owned application, maintaining data and resolving data issues through direct on-line access and/or requests to the department for direct database changes.

E. Information Technology (IT) Modernization

Information Technology Modernization includes the purchase of planned or directed changes in technical sophistication application systems and equipment.

1. The provider may purchase new or replacement IT in accordance with policy and procedures listed in the Community-Based Care Authority and Requirements Reference Guide.
2. Replacement of department furnished IT necessary in the performance of this contract shall be procured by the provider and funded against payments made under this contract at no additional cost to the department.
3. The provider shall provide new or factory reconditioned parts and components when practicable in providing maintenance and repair services as described herein.
    a. All replacement units, parts, components and materials to be used in the maintenance and repair of equipment shall be compatible with existing equipment on which it is to be used and shall meet industry standards and be suitable for their intended use.
    b. If material that meets the accepted industry standard cannot be obtained, the provider must obtain the concurrence of the Region's Information Systems Director before using alternate materials.

F. Data Analytics

The department intends to establish guidelines and requirements that incorporate data analytics in improving service delivery to clients. Data analytics is the process of examining raw data with the purpose of drawing inferences or conclusions from that data. Data analytics should be used to allow case workers to make better business decisions for client services. Data analytics may involve the process of sorting through huge data sets using sophisticated software to identify undiscovered patterns and establish hidden relationships. The department may also deliver or require the use of applications performing data analytics. The provider shall update quarterly, annually, and biannually the data analytic system(s) as directed by the department, depending on the analytic and relevant cycle time for updates. The data analytic system(s) may report outcomes through one or more dashboards which should allow users to drill down for more granular information for that particular analytic.

G. Network Services

1. The department agrees to coordinate with the provider staff in the installation, configuration and security access to any state owned application(s).
2. The department agrees to coordinate with the provider staff to resolve WAN access to any required state application(s).
3. Provider staff may optionally call the Customer Assistance Center in Tallahassee for first line of support for Department applications. All such IT support will be documented by means of a generated work order by the department.
4. The department reserves the right to charge for Customer Assistance Center calls that are caused by failure of provider-owned equipment outside that approved by the department or incorrect operation of the provider's equipment.
5. Provider staff will troubleshoot all LAN/WAN connections. If any LAN connection requires repair or replacement, then it is the responsibility of the provider to pay for these repairs or replacements.
6. The department shall provide network security for State-owned applications. The provider shall provide PC software and network security software products and access assistance to provider staff for non-State-owned applications. Example: Seagull Corporation's BlueZone software.
7. The provider shall provide network security software products and access assistance to the provider staff for all applications.
8. The Provider must provide a network diagram outlining the connectivity to Covered Data and all department resources.
9. The Provider shall maintain supported and patched operating systems.
10. The Provider shall provide all external facing IP addresses including internet facing connections and department facing connections.
11. The Provider agrees to vulnerability scanning and penetration testing.
12. Wireless LAN Connectivity:
    a. All wireless traffic must have a minimum encryption of 128 bits, WEP and WPA are not sufficient protocols for encrypting traffic.