MEMORANDUM OF UNDERSTANDING REGARDING RECORDS SHARING FOR SYNCHRONIZATION OF SERVICES

1) PURPOSE

a) The Parties enter into this Memorandum of Understanding (MOU) to facilitate the development and ongoing inter-agency implementation of an integrated client database, intended to improve the administration of certain services amongst clients who receive or may receive these services from one or more programs. Development and implementation of the integrated database requires that the Agency Parties make specific governmental records available to the Utah Governor's Office of Management and Budget (GOMB) and Utah Department of Technology Services (DTS) to be integrated into the database. This MOU sets out the terms and conditions for the provision, sharing, and authorized use of the records maintained in the integrated database.

b) The Parties assert that the providing and sharing of records is necessary to accomplish the intended benefits of the integrated system, which are mutually beneficial to the Agency Parties, individual clients, and to the public. The Parties agree that the ongoing use of the integrated database may improve the individual and joint performance of governmental functions by:

i) Sharing client information within the integrated database allowing service providers to communicate holistically about clients in common,

ii) Serving state agency clients through a unified service team that minimizes redundancy and/or conflict,

iii) Designing service/case plans based on the capacity of the clients,

iv) Prioritizing and unifying the primary objectives of case plans,

v) Providing access to real-time information on the progress of planned objectives amongst service providers who have clients in common,

vi) Facilitating the achievement of client objectives more frequently upon the first attempt,

vii) Reducing client lengths of service for each program,

viii) Reducing client waiting times for services, and

ix) Identifying and resolving program-specific bottlenecks and those found between service providers more efficiently.

2) PARTIES

a) The Parties to this MOU are: The Utah Department of Corrections (UDC), the Utah Department of Human Services (DHS), and the Utah Department of Workforce Services (DWS), together referred to herein as the "Agency Parties," the Utah Governor's Office of Management and Budget (GOMB) and the Utah Department of Technology Services (DTS), together referred to herein as the "Administrative Parties." Each of the Parties to this MOU is a governmental entity as defined in the Utah Government Records Access Management Act, 63G-2-103(11) ("GRAMA").

3) DATABASE INTEGRATION, IMPLEMENTATION, AND USE

a) Subject to the disclosure, use, and data security requirements stated in this MOU, and subject to applicable federal and state law, each of the Agency Parties will provide respective records from specific programs to GOMB and DTS for integration into the database as follows:

i) UDC will provide current client records as maintained in the O-Track information system.

ii) DHS will provide current client records for:

(1) Division of Juvenile Justice Services (DJJS) clients who are receiving services pursuant to an active Youth and Family Plan, as maintained in the CARE information system, and

(2) Division of Child and Family Services (DCFS) clients who are receiving services pursuant to an active in-home Child and Family Plan or an out-of-home Child and Family Plan with a permanency goal of Reunification, Remain Home, or Individualized Permanency, as maintained in the SAFE information system.

iii) DWS will provide current client records for:

(1) The Family Employment Program (FEP) clients, as maintained in the UWORKS information system, and

(2) Vocational Rehabilitation (VR) clients, as maintained in the AWARE information system.

b) Records provided from all the aforementioned programs to the database may include but are not limited to:

i) Client personally identifiable information, which includes but is not limited to name(s), date(s) of birth, address(es), phone number(s), social security number(s), race, ethnicity, and gender.

ii) Other unique identifiers such as case ID, client ID or offender ID, and classifications such as case type.

iii) Associated case managers/worker information, which includes but is not limited to name(s), contact information, supervisor name(s), supervisor contact information, and their respective clients as currently assigned.

c) Records provided from only the UDC and DWS programs to the database include:

i) Client service/case plan components, which include but are not limited to client goals, associated dates, activities, progress indicators, risk factors, assessment information, and associated notes.

4) RECORDS SHARING, USE AND SECURITY

a) Sharing

i) The Parties to this MOU enter into and shall perform this MOU in compliance with applicable state and federal law. All records integrated into the database are governmental records and are variously classified under GRAMA as "private," "protected," or "confidential." The inter-agency sharing and use of such records are subject to the requirements of GRAMA and may be subject to federal law including, 45 CFR 205.50; 34 CFR 361.38; 34 CFR 99.30; 42 CFR part 2; HIPAA; 5 USC 552; 42 USC 1306; 20 CFR 401.150.

ii) The Parties share their respective records pursuant to the MOU under the authority of GRAMA, U.C.A. 63G-2-206(2)(a). Pursuant to that statute, the Parties hereby assert that: (a) such records are necessary to the performance of each Parties' respective governmental duties and functions; (b) that the records shared and received will be used for purposes similar to the purposes for which such records were collected and maintained; and (c) that the use of such records will produce a public benefit greater or equal to the individual privacy right that protects such records.

iii) Each party acknowledges that, as an authorized user of the integrated database, they are under the same obligations and restrictions governing access, confidentiality, use, and dissemination of such records required under GRAMA, UCA63G-2-part 3 and other applicable laws.

b) Use

i) As allowed by law, the Agency Parties will obtain express consent from the clients, or individual service recipients, before making their personally identifiable and restricted records available to the other Parties from the integrated database. As such, access to the integrated database and the records maintained therein shall be made available only to the Parties' authorized employees and agents, their supervisors, or others with an operational or legal need who are directly involved in administering a service program or plan to the client of record, or who are expressly assigned to maintain, administer, and support the database.

(1) Once express consent from the client has been received, for as long as that express consent remains valid, the client's records may be extracted for the following uses and presentations:

(a) By the authorized users of Agency Parties for integration back into their respective information systems and made available to the authorized employees, personnel, or agents with an operational need.

(b) By the authorized users of Administrative Parties in a secure interface accessible to authorized employees, personnel, or agents from any of the Agency Parties with an operational need.

(c) If express consent from the client has been rescinded, the client's records may no longer be extracted for the aforementioned uses and presentations until such time as the client resubmits express consent.

(2) The aggregated, de-identified records may be extracted for the following uses and presentations:

(a) By the Parties or their agents in a secured interface accessible to authorized employees, personnel, or agents from any of the Parties with an operational need.

(3) All client and case management records as detailed herein will be maintained in the integrated database as historical, longitudinal information. However, the provided client information will be removed from the integrated database upon receipt of a valid expungement through either: (1) a court order for a UDC criminal offender, or (2) a court order or a DCFS process for a DCFS client.

c) Security

i) SECURE PROTECTION AND HANDLING OF DATA: If authorized users are given access to Data, the protection of the Data shall be an integral part of the business activities of the Parties, and the Parties shall ensure that there is no inappropriate or unauthorized use of Data. The Parties shall safeguard the confidentiality, integrity, and availability of the State Data and comply with the conditions outlined below. The Parties reserve the right to verify adherence to the following conditions to ensure they are met:

(1) Network Security: DTS shall maintain network security that, at a minimum, includes: network firewall provisioning, intrusion detection, and regular third-party penetration testing. DTS shall maintain network security and

ensure that the Parties network security policies conform to one of the following:

(a) Those standards the State of Utah applies to its own network, found outlined in DTS Policy 5000-0002 Enterprise Information Security Policy;

(b) Current standards set forth and maintained by the National Institute of Standards and Technology, includes those at: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf; or

(c) Any generally recognized comparable standard that the Parties then applies to its own network and pre-approved by DTS in writing.

(2) State Data Security: The Parties shall protect and maintain the security of State Data with protection that is at least as good as or better than that maintained by the State of Utah as identified in DTS Policy 5000-0002. These security measures included but are not limited to maintaining secure environments that are patched and up to date with all appropriate security updates as designated (ex. Microsoft Notification). Administrative Parties are responsible for defining, implementing, and maintaining of the security measures on the integrated database and any associated systems or interfaces that meet the terms of this MOU. Agency Parties are responsible for defining, implementing, and maintaining of the security measures associated with any data received from the integrated database that meet the terms of this MOU.

(3) State Data Transmission: DTS shall ensure all transmission or exchange of system application data with DTS and State of Utah and/or any other parties expressly designated by the State of Utah, shall take place via secure means (ex. HTTPS or FTPS).

(4) State Data Storage: All State Data will be stored and maintained in data centers in the United States. No State Data will be processed on or transferred to any portable or laptop computing device or portable storage medium, except for devices that are used and kept only at DTS managed data centers, unless such medium is part of the Parties designated backup and recovery process.

(5) Access: The Parties shall permit employees and Subcontractors to remotely access Data only as required to provide technical support.

(6) State Data Encryption: The Parties shall store all data provided to employees and contractors, as well as any backups made of that data, in encrypted form using no less than 128 bit key and include all data as part of a designated backup and recovery process.

(7) Password Protection: Any portable or laptop computer that has access to data shared per this MOU shall be equipped with strong and secure password protection.

(8) State Data Re-Use: All data exchanged shall be used expressly and solely for the purpose enumerated in this MOU. No Data of any kind may be transmitted, exchanged, or provided to other contractors or third parties except on a case-by-case basis as specifically agreed to in writing by DTS and the Parties who own the data.

(9) State Data Destruction: Upon expiration or termination of this MOU, the Parties shall erase, destroy, and render unreadable all shared Data from all computer systems and backups, and certify in writing that these actions have been completed within thirty (30) days of the expiration or termination of this MOU or within seven (7) days of the request of DTS, whichever shall come first, unless DTS provides the Parties with a written directive. DTS's written directive may require that certain data be preserved in accordance with applicable law.

ii) SECURITY INCIDENT OR DATA BREACH NOTIFICATION: The Parties shall immediately inform DTS of any Security Incident or Data Breach. It is within DTS's discretion to determine whether any attempted unauthorized access is a Security Incident or a Data Breach.

(1) Incident Response: The Parties may need to communicate with outside entities regarding a Security Incident, which may include contacting law enforcement and seeking external expertise as mutually agreed upon, defined by law or contained in this MOU. Discussing Security Incidents with DTS should be handled on an urgent as-needed basis, as part of the Parties communication and mitigation processes, defined by law or contained in this MOU.

(2) Security Incident Reporting Requirements: The Parties shall promptly report a Security Incident to DTS.

(3) Breach Reporting Requirements: As required by Utah Code 13-44-202 or any other law, the Parties shall immediately notify DTS of a Data Breach that affects the security of State Data.

iii) DATA BREACH RESPONSIBILITIES: The Parties shall comply with all applicable laws that require the notification of individuals in the event of a Data Breach or other events requiring notification in accordance with DTS Policy 5000-0002 Enterprise Information Security Policy. In the event of a Data Breach or other event requiring notification under applicable law (Utah Code § 13-44-101 thru 301 et al), the Parties shall: (a) cooperate with DTS and other Parties by sharing information relevant to the Data Breach; (b) promptly implement necessary remedial measures, if necessary; and (c) document responsive actions taken related to the Data Breach, including any post-incident review of events and actions taken to make changes in business practices in relation to the Data Breach. If the Data Breach requires public notification, all communication shall be coordinated with DTS and the owner/source of the Data. The Party that is responsible for the breach is responsible for all notification and remedial costs and damages.

5) OTHER TERMS AND ACKNOWLEDGEMENT

a) This MOU will take effect on signing of the parties and, subject to later amendment, will remain in effect until terminated or the Parties enter into a separate, superseding MOU governing the ongoing data sharing, and inter-agency use of the integrated blueprint database.

b) Any Party to this MOU may request review and amendment of this MOU upon written approval of the Agency contact. Nothing in this MOU shall be construed as a waiver of any rights, protections, defenses, or immunities provided under the Utah Governmental Immunity Act., UCA 63G-7-101 et seq.

6) CONTACT PERSONS

DWS
Greg Paras
Deputy Director
801-526-9313

UDC
Julie Christenson
Director, Research & Planning
801-907-1467

DHS
Mark Brasher
Deputy Director
801-538-4104

GOMB
Rachel Stone
Chief Data Officer
801-538-1516

DTS
Dan Frei
Finance Director
801-538-3459

7) SIGNATURES

Greg Paras
Greg Paras (Mar 5, 2020)
DWS

Mark Brasher
Mark Brasher (Mar 6, 2020)
DHS

julie christenson
UDC

Dan Frei (Mar 6, 2020)
DTS

Rachel Stone
Rachel Stone (Mar 6, 2020)
GOMB