06/21/2018

# DTD Data Privacy Framework

## Introduction

*Driving the Dream* (DTD), and the United Way of the Mid-South (UWMS), are committed to providing the highest levels of operational privacy and confidentiality to all individuals served through our network of Referral Partners and Care Coordination Hubs. It must be acknowledged that these individuals are often members of various, often multiple, vulnerable populations, and that our current atmosphere is one of facile information sharing, rampant cyber-intrusions, and increased institutional discrimination. It is rare that one spends time watching or reading the news without mention of data being leaked, hacked, or shared inappropriately. It is to our benefit to become more security-conscious, and it is the intention of DTD to assure our partners and our community that we are actively engaged in vigorously protecting the information entrusted to us.

As a part of providing this assurance, DTD has partnered with CoactionNet, our database vendor, to prepare this framework describing the technology, policy, and processes in place to provide robust privacy protections for all associated individuals. This framework represents a thoroughly vetted, yet ever-evolving, set of principles and practices set forth by DTD based on industry best practices and feedback from our partner agencies. If your questions and concerns are not addressed in this framework, or you would like to engage in the continuous conversation regarding data privacy and DTD, please contact Eric Burden (eric.burden@uwmidsouth), Data and Quality Improvement Manager for *Driving the Dream.*

# Technology

Foundational to any description of data protections are the security protocols and technological implementations that underpin the transmission, retrieval, and storage of data. CoactionNet (and Apricot, the platform upon which CoactionNet is built), address this through the highest-level industry standards for encryption, both in transit and at rest.

In transit, data is encrypted using what is known as an AES-256 cipher[1] over a TLS 1.2 protocol[2] connection. This level of encryption is considered by the US federal government to be more than adequate to encrypt communications classified at the TOP SECRET level[3], in accordance with Federal Information Processing Standards, and reviewed by the National Security Agency. In practice, this means that every piece of data sent from a computer to the CoactionNet database and back is broken into small bits, and each bit is strongly encrypted. This prevents anyone on your network who might intercept your internet traffic (including your employer or ISP) from being able to read what has been transmitted. Additionally, CoactionNet traffic is restricted to this secured pathway, any attempt to communication with CoactionNet over a non-secure channel is refused.

Data stored in the CoactionNet database is also encrypted, this time using a 2048-bit RSA key.[4] This, again, is the highest level of industry standard encryption, utilized by a variety of industry leaders. It has been estimated that brute-force hacking a 2048-bit RSA key, utilizing currently available technology, would take hundreds of thousands of times longer than the current age of the universe.[5] This means that if the computers housing the information were ever stolen, the information stored on them would be useless to anyone attempting to read that information. This event is also extremely unlikely, as CoactionNet data is stored using services provided by Amazon Web Services (AWS), the largest provider of cloud web services. AWS has an excellent reputation, and is utilized by such major corporations as GE and Intuit, startups like AirBnB, a number of banks, and federal agencies such as the FDA and CDC.[6]

[1] https://en.wikipedia.org/wiki/Advanced_Encryption_Standard
[2] https://en.wikipedia.org/wiki/Transport_Layer_Security
[3] https://csrc.nist.gov/csrc/media/projects/cryptographic-module-validation-program/documents/cnss15fs.pdf
[4] https://en.wikipedia.org/wiki/RSA_(cryptosystem)
[5] https://www.digicert.com/TimeTravel/math.htm
[6] https://aws.amazon.com/solutions/case-studies/

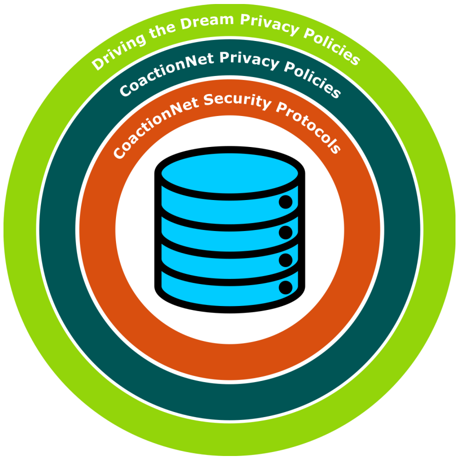
# Policy

Both CoactionNet and DTD have instituted policies regarding confidentiality, proper use of data, data exfiltration remediation, and improper or unauthorized releases of confidential information. For CoactionNet, that includes the CoactionNet User Agreement[7], the CoactionNet Privacy Policy[8], and the CoactionNet Data Breach Policy[9]. These documents, as well as the DTD Privacy Policy[10], are available for review upon request and should be included in any dissemination of this framework. In brief, these policies provide that:

- Users must make specific, reasonable efforts to ensure the confidentiality of data entered into CoactionNet, including: management of any hard copies of materials, safekeeping user credentials, limiting access to necessary information, and promptly alerting CoactionNet to any suspected or confirmed improper release or misuse of data.
- Sharing of data with any third party is strictly limited to a narrow set of acceptable uses, with stipulations for maintenance of confidentiality.
- Responses to any suspected release of information, either by a partner or through external acquisition, shall include: halting the release, data recovery, assessment of the scope of the release, notification of affected parties, incident and response evaluation.

DTD maintains a privacy policy in addition to those maintained by CoactionNet, which is intended to strengthen and support the protections provided by CoactionNet. In brief, this policy provides that:

- *Driving the Dream* data is narrowly defined, and all data sharing and acceptable use is limited to that which is affirmatively consented to.
- Any suspected improper release of information be promptly reported to DTD staff.
- Data sharing or use outside that defined by the privacy policy is strictly prohibited, and will trigger a robust set of responses from DTD staff, including: incident reporting to CoactionNet, development of a shared impact assessment, and performance of an ethics review in the event that data was released from a partner agency or registered CoactionNet user.

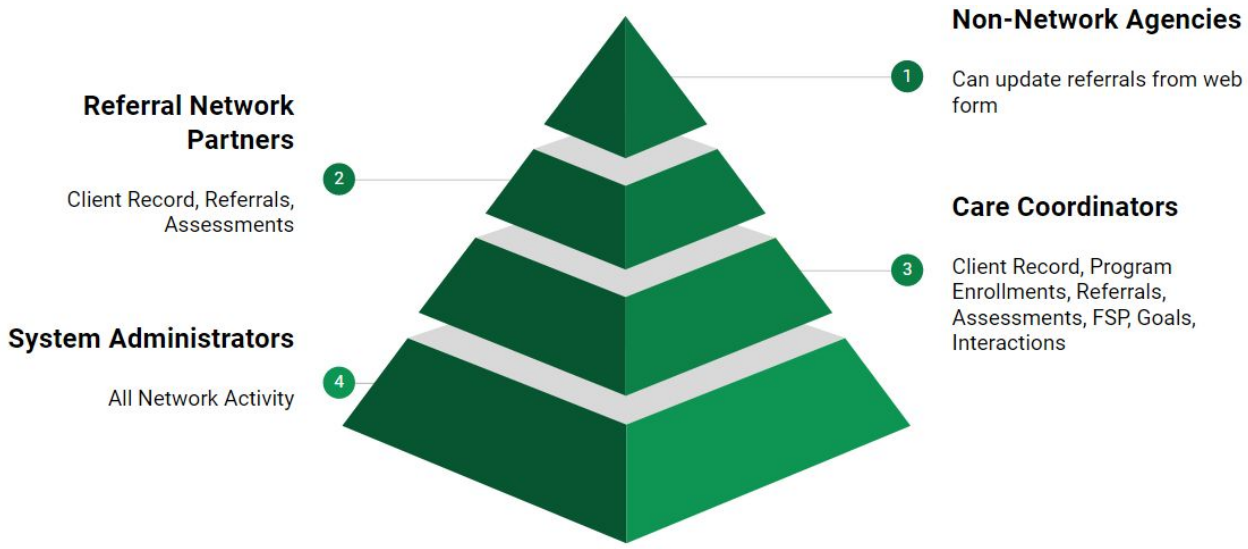

Driving the Dream Privacy Policies
CoactionNet Privacy Policies
CoactionNet Security Protocols

[7] Appendix A
[8] Appendix B
[9] Appendix C
[10] Appendix D

# Process

The processes and practices related to *Driving the Dream* have been developed with confidentiality as a major touchstone, such that any data entered into CoactionNet is properly segmented and access is restricted to those users whose completion of responsibilities rely on such access. A full description of these processes is included in the training materials provided to DTD/CoactionNet users prior to granting such users with credentials for accessing CoactionNet, as well as the CoactionNet User Guide which is available from the DTD Knowledge Base.[11] In brief, *Driving the Dream* is designed such that:

- Out-of-Network service providers who receive a referral from DTD have no access to any client information that is not specifically included in the referral.
- Each referral for services requires an informed consent from the client.[12]
- Referral Network partners have access limited to Client Records, Referral history (including disposition of the referrals), and optional assessments.
- Care Coordination Hub partners have access limited to Client Records, Referral history (including disposition of the referrals), optional assessments, Program Enrollments, Case Goals, Family Success Plans, and Client Interactions.
- System Administrators have access to all *Driving the Dream* data.
- Information collected at intake is reduced to the bare minimum required to provide analysis and reporting of DTD outcomes consistent with DTD's programmatic obligations and to analyze performance in order to improve client outcomes.


Non-Network Agencies
1
Can update referrals from web form
Referral Network Partners
2
Client Record, Referrals, Assessments
Care Coordinators
3
Client Record, Program Enrollments, Referrals, Assessments, FSP, Goals, Interactions
System Administrators
4
All Network Activity

[11] DTD Knowledge Base will be formally launched on July 11th, 2018

[12] Referral and Program Enrollment Consent Forms, Appendix E

# Appendix A

## CoactionNet User Agreement

CoactionNet **USER AGREEMENT**

## STATEMENT OF CONFIDENTIALITY AND REQUEST FOR END USER LICENSE

**Name: ____________________________________________________________**
(Please print clearly.)

**Email Address: _____________________________________________________**
(Please print clearly.)

Training: [ ] by "Agency" Internal Staff, [X] by CoactionNet Sys Admin, and/or [ ] via Training Webinar created by CoactionNet staff.

Name(s) and date(s) of trainings completed: ___TBD_____________________________________

**Important**
Please note this form must be completed by new users and existing users on an annual basis.
If you have any questions regarding the completion of this request, please contact Dottie Jones (using email below or call 901-833-5808).
After filling out this form and adding appropriate signatures, scan and email to:
Dottie.Jones@CoactionNet.org

### STATEMENT OF CONFIDENTIALITY

I AGREE TO MAINTAIN THE STRICT CONFIDENTIALITY OF INFORMATION OBTAINED THROUGH the CoactionNet system. This information will be used only for legitimate client services and administration of the above named agency. Any breach of confidentiality will result in immediate termination of participation in CoactionNet.

### TRAINING

I agree to attend all required training sessions, as deemed appropriate by the System Administrator(s) and/or other CoactionNet staff.

Signature: _________________________________________________ Date: _______________

### REQUEST FOR LICENSE

Each user requires a unique username and password, which is to be kept private. Use of another user's username (account) is grounds for immediate termination from CoactionNet.

### USER'S RESPONSIBILITY STATEMENT

Your username and password give you access to CoactionNet. Initial each item below to indicate your understanding of the proper use of your username and password, and sign where indicated. Any failure to uphold the confidentiality standards set forth below is grounds for immediate termination from CoactionNet.

# CoactionNet USER AGREEMENT

*Initial Only*

____ I understand that I must take all reasonable means to protect personal information that is in hard copy format, including, but not limited to, reports, data entry forms, and signed consent forms.

____ I understand those hard copies of CoactionNet information must be kept in a secure file.

____ I understand that once the hard copies of CoactionNet are no longer needed, they must be properly destroyed to maintain confidentiality.

____ I understand that I must take all reasonable means to protect personal information that is stored within the application, including, but not limited to, usage on a network, desktop, laptop, and external storage drive.

____ I understand that I must take all reasonable means to keep my password physically secure.

____ I understand that my username and password are for my use only and should not be shared with any other user.

____ I understand that the only individuals who can view CoactionNet information are authorized users and the clients to whom the information pertains.

____ I understand that I may only view, obtain, disclose, or use the database information that is necessary in performing my job.

____ I understand that these rules apply to all users of the CoactionNet whatever their work role or position.

____ I understand that if I notice or suspect a security breach, I must immediately notify the CoactionNet Administrator.

**I understand and agree to the above statements.**

**User Signature: ______________________________ Date: ____________________**

– – – – – – – – – – – – – – – – – – – – – – – – – – – – – – – – – – – – – – – – – – – – –

To be completed by the CoactionNet Administrator:
[ ] Yes [ ] No Verified user was HIPAA trained (per agency specific requirements).
[ ] Yes [ ] No Verified user was Agency or CoactionNet application trained
[ ] Yes [ ] No Added user’s business email to the CoactionNet Tracking list
[ ] Yes [ ] No Submitted request to add CoactionNet ID
__________ Provider ID number for default program
__________ Provider ID number(s) for all other programs

User ID (Assigned by CoactionNet): ____________________________________________

CoactionNet Admin Signature:________________________ Date: ____________________

# Appendix B

## CoactionNet Privacy Policy

# CoactionNet Privacy Policy

Protecting your private information is our priority. This Statement of Privacy applies to https://apricot.socialsolutions.com/ and www.coactionnet.org and Wraparound Shelby, Inc. DBA CoactionNet and governs data collection and usage. For the purposes of this Privacy Policy, unless otherwise noted, all references to Wraparound Shelby, Inc. DBA CoactionNet include https://apricot.socialsolutions.com/ and www.coactionnet.org and CoactionNet/Apricot. The CoactionNet/Apricot website is a social services case management site. By using the CoactionNet/Apricot website, you consent to the data practices described in this statement.

**Collection of your Personal Information**
In order to better provide you with products and services offered on our Site, CoactionNet/Apricot may collect personally identifiable information, such as your:

- First and Last Name
- Mailing Address
- E-mail Address
- Phone Number
- Employer
- Job Title

CoactionNet/Apricot may also collect anonymous demographic information, which is not unique to you, such as your:

- Age
- Gender
- Race
- Household Income
- Other information as requested by member organizations

We do not collect any personal information about you unless you consent and voluntarily provide it to us. However, you may be required to provide certain personal information to us when you elect to use certain products or services available on the Site. These may include: (a) registering for an account on our Site; (b) sending us an email message. To wit, we will use your information for, but not limited to, communicating with you in relation to services and/or products you have requested from us. We also may gather additional personal or non-personal information in the future.

**Use of your Personal Information**
CoactionNet/Apricot collects and uses your personal information to operate its website(s) and deliver the services requested.

CoactionNet/Apricot may also use your personally identifiable information to inform you of other products or services available from CoactionNet/Apricot and its affiliates.

**Sharing Information with Third Parties**
CoactionNet/Apricot does not sell, rent or lease its customer lists to third parties.

CoactionNet/Apricot may share data with trusted partners to help perform statistical analysis, send you email or postal mail, or provide customer support. All such third parties are prohibited from using your personal information except to provide these services to CoactionNet/Apricot, and they are required to maintain the confidentiality of your information.

CoactionNet/Apricot may disclose your personal information, without notice, if required to do so by law or in the good faith belief that such action is necessary to: (a) conform to the edicts of the law or comply with legal process served on CoactionNet/Apricot or the site; (b) protect and defend the rights or property of CoactionNet/Apricot; and/or (c) act under exigent circumstances to protect the personal safety of users of CoactionNet/Apricot, or the public.

**Automatically Collected Information**
Information about your computer hardware and software may be automatically collected by CoactionNet/Apricot. This information can include: your IP address, browser type, domain names, access times and referring website addresses. This information is used for the operation of the service, to maintain quality of the service, and to provide general statistics regarding use of the CoactionNet/Apricot website.

**Use of Cookies**
The CoactionNet/Apricot website may use "cookies" to help you personalize your online experience. A cookie is a text file that is placed on your hard disk by a web page server. Cookies cannot be used to run programs or deliver viruses to your computer. Cookies are uniquely assigned to you, and can only be read by a web server in the domain that issued the cookie to you.

One of the primary purposes of cookies is to provide a convenience feature to save you time. The purpose of a cookie is to tell the Web server that you have returned to a specific page. For example, if you personalize CoactionNet/Apricot pages, or register with CoactionNet/Apricot site or services, a cookie helps CoactionNet/Apricot to recall your specific information on subsequent visits. This simplifies the process of recording your personal information, such as billing addresses, shipping addresses, and so on. When you return to the same CoactionNet/Apricot website, the information you previously provided can be retrieved, so you can easily use the CoactionNet/Apricot features that you customized.

You have the ability to accept or decline cookies. Most Web browsers automatically accept cookies, but you can usually modify your browser setting to decline cookies if you prefer. If you choose to decline cookies, you may not be able to fully experience the interactive features of the CoactionNet/Apricot services or websites you visit.

**Links**
The CoactionNet.org website contains links to other sites. Please be aware that we are not responsible for the content or privacy practices of such other sites. We encourage our users to be aware when they leave our site and to read the privacy statements of any other site that collects personally identifiable information.

**Security of your Personal Information**
CoactionNet/Apricot secures your personal information from unauthorized access, use, or disclosure. CoactionNet/Apricot uses the following methods for this purpose:

- SSL Protocol

When personal information is transmitted to other websites, it is protected through the use of encryption, such as the Secure Sockets Layer (SSL) protocol.

We strive to take appropriate security measures to protect against unauthorized access to or alteration of your personal information. Unfortunately, no data transmission over the Internet or any wireless network can be guaranteed to be 100% secure. As a result, while we strive to protect your personal information, you acknowledge that: (a) there are security and privacy limitations inherent to the Internet which are beyond our control; and (b) security, integrity, and privacy of any and all information and data exchanged between you and us through this Site cannot be guaranteed.

**Children Under Thirteen**
CoactionNet/Apricot collects personally identifiable information from children under the age of thirteen. CoactionNet/Apricot collects this information for the following reason(s): As required by member organizations and only with parental consent.

If you are a parent and you have questions regarding our data collection practices, please contact us using the information provided at the end of this Statement of Privacy.

**External Data Storage Sites**
We may store your data on servers provided by third party hosting vendors with whom we have contracted.

**Statement of Confidentiality**
All approved users of Coacti0onNet/Apricot sign a User Agreement that specifically states the following:

> I AGREE TO MAINTAIN THE STRICT CONFIDENTIALITY OF INFORMATION OBTAINED THROUGH the CoactionNet system. This information will be used only for legitimate client services and administration. Any breach of confidentiality will result in immediate termination of participation in CoactionNet.

Users also agree to the following:

- I understand that I must take all reasonable means to protect personal information that is in hard copy format, including, but not limited to, reports, data entry forms, and signed consent forms.

- I understand those hard copies of CoactionNet information must be kept in a secure file.

- I understand that once the hard copies of CoactionNet are no longer needed, they must be properly destroyed to maintain confidentiality.

- I understand that I must take all reasonable means to protect personal information that is stored within the application, including, but not limited to, usage on a network, desktop, laptop, and external storage drive.

- I understand that I must take all reasonable means to keep my password physically secure.

- I understand that I should not 'save' my password in my browser program.

- I understand that my username and password are for my use only and should not be shared with any other user.

- I understand that the only individuals who can view CoactionNet information are authorized users and the clients to whom the information pertains.

- I understand that I may only view, obtain, disclose, or use the database information that is necessary in performing my job.

- I understand that these rules apply to all users of the CoactionNet whatever their work role or position.

- I understand that if I notice or suspect a security breach, I must immediately notify the CoactionNet Administrator.

User Agreements are updated on an annual basis.

**Changes to this Statement**
CoactionNet/Apricot reserves the right to change this Privacy Policy from time to time. We will notify you about significant changes in the way we treat personal information by sending a notice to the primary email address specified in your account, by placing a prominent notice on our site, and/or by updating any privacy information on this page. Your continued use of the

Site and/or Services available through this Site after such modifications will constitute your: (a) acknowledgment of the modified Privacy Policy; and (b) agreement to abide and be bound by that Policy.

**Contact Information**

CoactionNet/Apricot welcomes your questions or comments regarding this Statement of Privacy. If you believe that CoactionNet/Apricot has not adhered to this Statement, please contact CoactionNet/Apricot at:

Wraparound Shelby, Inc. DBA CoactionNet
1005 Tillman
Memphis, Tennessee 38112

Email Address:
dottie.jones@coactionnet,org

Telephone number:
901-833-5808

Effective as of May 1, 2018

# Appendix C

## CoactionNet Data Breach Policy

# CoactionNet Data Breach Policy

## 1. Overview

Data breaches are increasingly common occurrences whether caused through human error or malicious intent. CoactionNet operations rely on the proper use of Confidential Information and Personally Identifiable Information (PII) on a daily basis. Managing risk and responding in an organized way to Incidents and Breaches is key to operations.

## 2. Purpose

CoactionNet must have a robust and systematic process for responding to reported data security Incidents and Breaches. This policy is designed to standardize the CoactionNet-wide response to any reported Breach or Incident, and ensure that they are appropriately logged and managed in accordance with best practice guidelines. Standardized processes and procedures help to ensure the CoactionNet can act responsibly, respond effectively, and protect its information assets to the extent possible.

## 3. Scope

This policy applies to all CoactionNet staff, users and member organizations.

## 4. Policy

### A. GENERAL INFORMATION

A "Data Security Incident" or "Incident' shall mean an accidental or deliberate event that results in or constitutes an imminent threat of the unauthorized access, loss, disclosure, modification, disruption, or destruction of communication or information resources of the CoactionNet.

Common examples of data security Incidents include, but are not limited to, any of the following:

- Successful attempts to gain unauthorized access to a CoactionNet system or PII regardless of where such information is located
- Unwanted disruption or denial of service
- The unauthorized use of a CoactionNet system for the processing or storage of Confidential Information or PII
- Changes to CoactionNet system hardware, firmware, or software characteristics without the CoactionNet's knowledge, instruction, or consent
- Loss or theft of equipment where Confidential Information or PII is stored
- Unforeseen circumstances such as a fire or flood that could lead to the loss or misuse of Confidential Information or PII
- Human error involving the loss or mistaken transmission of Confidential Information or PII
- Hacking, social engineering, phishing or other subversive attacks where information is obtained by deceitful practice

A “Data Security Breach” or “Breach” is any Incident where CoactionNet cannot put in place controls or take action to reasonably prevent the misuse of Confidential Information or PII. A Breach is also an Incident where data has been misused.

Adopting a standardized and consistent approach to Incident management shall ensure that:

- Incidents are reported in a timely manner and can be properly investigated
- Incidents are handled by appropriately authorized and skilled personnel
- Appropriate levels of management are involved in response management
- Incidents are recorded and documented
- Organizational impacts are understood and action is taken to prevent further damage
- Evidence is gathered, recorded, and maintained in a form that will withstand internal and external scrutiny
- External agencies, customers, and data users are informed as required
- Incidents are dealt with in a timely manner and normal operations are restored
- Incidents are reviewed to identify improvements in policies and procedures

Incidents can occur locally, in the cloud, or through third party service providers. Reporting and management of Incidents shall occur similarly. Third party providers shall also be governed by contract terms and liability as defined in their operational agreements.

## B. DATA CLASSIFICATIONS

Incidents vary in impact and risk depending on a number of mitigating factors including the content and quantity of the data involved. It is critically important that CoactionNet management respond quickly and identify the data classification of the Incident. This allows staff to respond accordingly in a timely and thorough manner.

All reported Incidents shall be classified as below in order to assess risk and approaches to mitigate the situation. Data classification shall refer to the following CoactionNet data categories:

**Public Data** - Information intended for public and community use or information that can be made public without any negative impact on the CoactionNet or its customers. Client PII shall never be considered public data unless the data is Directory Information as defined by CoactionNet policy.

**Confidential/Internal Data** - Information of a more sensitive nature to the business and educational operations of CoactionNet. This data represents basic intellectual capital, applications, and general knowledge. Access shall be limited to only those people that need to know as part of their role within the CoactionNet. Employee and Educator PII (with the exception of Social Security Numbers (SSN), financial information, or other critical information) falls within this classification.

**Highly Confidential Data**- Information that, if breached, causes significant damage to CoactionNet operations, reputation, and/or business continuity. Access to this information should be highly restricted. Client PII falls into this category of data. Employee or Client Financial Information, Social Security Numbers, and other critical information also fall into this classification.

## C. INCIDENT REPORTING

The following process shall be followed when responding to a suspected Incident:

- Confirmed or suspected Incidents shall be reported promptly to CoactionNet at 901-833-5808 or at dottie.jones@coactionnet.org. A formal report shall be filed that includes full and accurate details of the Incident including who is reporting the Incident and what classification of data is involved.

- Once an Incident is reported, the director shall conduct an assessment to establish the severity of the Incident, next steps in response, and potential remedies and solutions. Based on this assessment, the director shall determine if this Incident remains an Incident or if it needs to be categorized as a Breach.

- All Incidents and Breaches will be centrally logged and documented to ensure appropriate documentation, oversight, and consistency in response, management, and reporting.

## D. CLASSIFICATION

Data Breaches or Incidents shall be classified as follows:

**Critical/Major Breach or Incident** – Incidents or Breaches in this category deal with Confidential Information or PII and are on a large scale (CoactionNet-wide). All Incidents or Breaches involving Client PII will be classified as Critical or Major. They typically have the following attributes:

- Any Incident that has been determined to be a Breach

- Significant Confidential Information or PII loss, potential for lack of business continuity, CoactionNet exposure, or irreversible consequences are imminent

- Negative media coverage is likely and exposure is high

- Legal or contractual remedies may be required

- Requires significant reporting beyond normal operating procedures

- Any breach of contract that involves the misuse or unauthorized access to Client PII

**Moderately Critical/Serious Incident** – Breaches or Incidents in this category typically deal with Confidential Information and are on a medium scale (e.g. <50 users on the internal network, application or database related, limited exposure). Incidents in this category typically have the following attributes:

- Risk to the CoactionNet is moderate

- Third party service provider and subcontractors may be involved

- Data loss is possible but localized/compartmentalized, potential for limited business continuity losses, and minimized CoactionNet exposure

- Significant user inconvenience is likely
- Service outages are likely while the breach is addressed
- Negative media coverage is possible but exposure is limited
- Disclosure of data is contained and manageable

**Low Criticality/Minor Incident** – Incidents in this category typically deal with personal or internal data and are on a small or individualized scale (e.g. <10 users on the internal network, personal or mobile device related). Incidents in this category typically have the following attributes:

- Risk to the CoactionNet is low
- User inconvenience is likely but not CoactionNet damaging
- Internal data released but data is not client, employee, or confidential in nature
- Loss of data is totally contained on encrypted hardware
- Incident can be addressed through normal support channels

## E. INCIDENT RESPONSE

Management response to any reported Incident shall involve the following activities:

**Assess, Contain and Recover Data** - All security Incidents shall have immediate analysis of the Incident and an Incident report completed by the Director or their designee. This analysis shall include a determination of whether this Incident should be characterized as a Breach. This analysis shall be documented and shared with the affected parties, and any other relevant stakeholders. At a minimum, the Director shall:

| Step | Action | Notes |
|---|---|---|
| A | Containment and Recovery: | Contain the breach, limit further organizational damage, seek to recover/restore data. |
| 1 | Breach Determination | Determine if the Incident needs to be classified as a Breach. |
| 2 | Ascertain the severity of the Incident or Breach and determine the level of data involved. | See Incident Classification |
| 3 | Investigate the Breach or Incident and forward a copy of the Incident report to the Director | Ensure investigator has appropriate resources including sufficient time and authority. If PII or confidential data has been breached, also contact the appropriate agencies and users. |

| | | |
|---|---|---|
| 4 | Identify the cause of the Incident or breach and whether the situation has been contained. Ensure that any possibility of further data loss is removed or mitigated as far as possible. If this loss cannot be mitigated, any Incident will be characterized as a Breach. | Compartmentalize and eliminate exposure. Establish what steps can or need to be taken to contain the threat from further data loss. Contact all relevant departments who may be able to assist in this process.<br>This may involve actions such as taking systems offline or restricting access to systems to a very small number of staff until more is known about the Incident. |
| 5 | Determine depth and breadth of losses and limit exposure/damages | Can data be physically recovered if damaged through use of backups, restoration or other means? |
| 6 | Notify authorities as appropriate | For criminal activities where property was stolen or fraudulent activity occurred, contact the appropriate authorities and general counsel. Should the Breach involve Client PII that involves a School Service Contract Provider, notify the CoactionNet Board members. |
| 7 | Ensure all actions and decisions are logged and recorded as part of incident documentation and reporting. | Complete Incident Report and file with Director |

**Assess Risk and Incident Scope** – All Incidents or Breaches shall have a risk and scope analysis completed by the Director or their designee. This analysis shall be documented and shared with the affected parties, and any other relevant stakeholders. At a minimum, the Director shall:

| B | Risk Assessment | Identify and assess ongoing risks that may be associated with the Incident or Breach. |
|---|---|---|
| 1 | Determine the type and breadth of the Incident or Breach | Classify Incident or Breach type, data compromised, and extent of breach |
| 2 | Review data sensitivity | Determine the confidentiality, scope and extent of the Incident or Breach. |
| 3 | Understand the current status of the compromised data | If data has been stolen, could it be used for purposes that harm the individuals whose identity has been compromised; If identity theft is involved, this poses a different type and level of risk. |
| 4 | Document risk limiting processes or technology components that contain and manage the Incident | Does encryption of data/device help to limit risk of exposure? |
| 5 | Determine what technologies or processes will mitigate the loss and restore service | Are there backups of the compromised data? Can they be restored to a ready state? |
| 6 | Identify and document the scope, number of users affected, and depth of Incident or Breach | How many individuals' personally identifiable information were affected? |
| 7 | Define individuals and roles whose data was compromised | Identify all clients, staff, districts, customers or vendors involved in the Incident or Breach |

| | | |
|---|---|---|
| 8 | If exploited, what will the compromised data tell a third party about the individual? Could it be misused? | Confidential Information or PII could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information could help a criminal build up a detailed picture associated with identity theft or fraud. |
| 9 | Determine actual or potential harm that could come to any individuals | Identify risks to individuals:<br>• Physical Safety<br>• Emotional Wellbeing<br>• Personal or Business Reputation<br>• Financial Implications<br>• Identity Concerns |
| 10 | Are there wider consequences to consider? | Is there risk to another organization, the state, or loss of public confidence? |
| 11 | Are there others who might provide support or advise on risks/courses of action? | Contact all local education providers, agencies, or companies impacted by the breached data, notify them about the Incident, and ask for assistance in limiting the scope of the Incident. |

**Notification and Incident Communications** - Each security Incident or Breach determined to be "moderately critical" or "critical" shall have communication plans documented by the CoactionNet senior leadership, and their designees to appropriately manage the Incident and communicate progress on its resolution to all effected stakeholders. At a minimum, the Director shall:

| C | Notification and Communications | Notification enables affected stakeholders to take precautionary steps and allow regulatory bodies to act on the Incident or Breach. |
|---|---|---|
| 1 | Are there legal, contractual or regulatory notification requirements associated with the Incident or Breach? | Review vendor contracts and compliance terms, assure state and federal reporting and notifications are understood. Secure appropriate legal advice as necessary to begin contractual adherence. |
| 2 | Notify impacted individuals of Incident or Breach remedies. | Provide individuals involved in the Incident or Breach with mitigation strategies to re-secure data (e.g. change user id and/or passwords etc.) |
| 3 | Determine Internal Communication Plans | Work with senior leadership and provide regular internal updates on status of Incident or Breach, remedies underway, and current exposure and containment strategies. This messaging should be provided to all internal state stakeholders and management. Messaging shall be coordinated through the Director's office. |

| | | |
|---|---|---|
| 4 | Determine Public Messaging | Prepare and execute a communication and follow-up plan with Director and senior leadership. Communication strategies need to define audience(s), frequency, messaging, and content. |
| 5 | Execute Messaging Plan | Working through the Director and appropriate leadership, execute the public and internal communication plans. Depending on the nature and scope of the Incident or Breach, multiple messages may need to be delivered as well as press and public communiques. Minimally notifications should include:<br>• A description of the Incident or Breach (how and when it occurred)<br>• What data was involved and whose data was compromised<br>• Details of what has been done to respond to the Incident or Breach and any associated risks posed<br>• Next-steps for stakeholders<br>• CoactionNet contacts for the Incident or Breach, any follow-, and other pertinent information<br>• When notifying individuals, provide specific and clear advice on the steps they can take to protect themselves and what the CoactionNet and/or third party vendor will do to help minimize their exposure<br>• Provide a way in which they can contact CoactionNet for further information or to ask questions about what has occurred (e.g. a contact name, helpline number or a web page) |

**Post Mortem Evaluation and Response** – Each Incident or Breach determined to be "moderately critical" or "critical" shall have a post mortem analysis completed by the Director and their designees to appropriately document, analyze, and make recommendations on ways to limit risk and exposure in the future. At a minimum, the Director shall:

| D | Evaluation and Response | To evaluate the effectiveness of the University's response to the Incident or Breach. |
|---|---|---|
| 1 | Establish where any present or future risks lie. | Assess and evaluate the root causes of the Incident or Breach and any ways to mitigate and/or prevent a similar occurrence. |

| | | |
|---|---|---|
| 2 | Consider the data and security measures employed. | Evaluate, analyze, and document the use cases and technical components of the Incident or Breach.  Document areas for improvement in environment, technology, or approach that limit future security exposures.  Make recommendations as appropriate. |
| 3 | Evaluate and identify areas of weakness in existing security measures and procedures. | Document lapses in process, procedure, or policy that may have caused the Incident or Breach.  Analyze and document solutions and remedies to reduce future risks. |
| 4 | Evaluate and  identify areas of weakness related to employee skills. | Assess employee readiness, education, and training.  Document and plan for updates in education or procedural changes to eliminate potential for future Incidents. |
| 5 | Report on findings and implement recommendations. | Prepare report and presentation to CoactionNet for major Incidents or Breaches. |

Each of these four elements shall be conducted as appropriate for all qualifying Incidents or Breaches. An activity log recording the timeline of Incident management shall also be completed. Reporting and documentation shall be filed and managed through the office of the Director.

## 5. Audit Controls and Management

On-demand documented procedures and evidence of practice should be in place for this operational policy. Appropriate audit controls and management practice examples are as follows:

- Archival completed Incident Reports demonstrating compliance with reporting, communication and follow-through.

- Executed communication plans for Incident management.

- Evidence of cross-departmental communication throughout the analysis, response and post-mortem processes.

## 6. Enforcement

Staff members, users or member organizations found in policy violation may be subject to disciplinary action, up to and including termination of access to CoactionNet and prosecution.

## 7. Distribution

This policy is to be distributed to all CoactionNet staff, users and member organizations.

# Appendix D

## Driving the Dream Privacy Policy

06/15/2018

# *Driving the Dream* Privacy Policy

## Core Philosophy

*Driving the Dream* aims to promote social progress and economic mobility by providing a framework by which social service agencies marshal resources and information in order to serve Clients in a coordinated and service-complete fashion. In doing so, *Driving the Dream* assumes the role of collector and distributor of potentially sensitive information, a role approached with the utmost care and consideration for the privacy rights of all individuals. This document outlines the practices related to safeguarding Client data as dictated by three core principles:

- Respect for individuals
- Respect for partner agencies
- A proactive approach

## Data Collection

Data is collected by partner agencies and entered into the CoactionNet database system. The owners and operators of the CoactionNet Database system also maintain privacy practices and policies; nothing in this document is intended to supersede any agreements that partner agencies have with CoactionNet directly. *Driving the Dream*, nor the United Way of the Mid-South, engages in direct collection of Client data for the *Driving the Dream* initiative. Data collection occurs at three distinct levels:

- Care Coordinators, employed at *Driving the Dream* Care Coordination Hubs, provide the highest level of direct engagement with Clients and therefore collect and enter the largest portion of accumulated data. These individuals provide direct case management services.

- Referral Network Partners collect less, and are engaged in sending and receiving referrals for direct services or Care Coordination.
- Non-partner agencies may receive referrals for services, and only provide data collection for the status of received referrals. The table below describes what Client data is collected, by whom, and for what purpose.

| **Data Collected** | **Collected by** | **Available to** | **Purpose** |
|---|---|---|---|
| Client Profile<br>● Name<br>● DOB<br>● Race<br>● Gender | ● Care Coordinators<br>● Referral Network Partners | ● System Administrators<br>● Care Coordinators<br>● Referral Network Partners | Provides the base Client record, under which all other data is collected. |
| Client Referral for Services<br>● Referring Organization<br>● Types of Services Provided<br>● Referring Organization (optional)<br>● Client Signature<br>● Client Contact Information<br>● Reasons for Referral<br>● Referral Program<br>● Referral Program Contact Information<br>● Notes<br>● Referral Status | ● Care Coordinators<br>● Referral Network Partners | ● System Administrators<br>● Care Coordinators<br>● Referral Network Partners | This data is transmitted with a referral for services, providing the recipient with the necessary information to enroll the Client. Referring organization information can be hidden in cases where this might be considered sensitive information, at the discretion of the agency entering the referral data. Data concerning referrals and outcomes is made available to Referral Network Partners and Care Coordinators as a way to manage service delivery across a variety of agencies/service domains. |
| Client Assessments<br>● Arizona Self-Sufficiency Matrix<br>● Herth Hope Index<br>● Adverse Childhood Experiences | ● Care Coordinators<br>● Referral Network Partners | ● System Administrators<br>● Care Coordinators<br>● Referral Network Partners | The collection of data associated with each of these assessments (included in Appendix A) is entirely optional and should be presented to Clients as such. Available data is included in aggregate outcome measures. |
| Program Enrollment<br>● Program Name<br>● Enrollment Date<br>● Program Site | ● Care Coordinators | ● System Administrators<br>● Care Coordinators | This data encapsulates the majority of the outcomes data associated with *Driving the Dream*. This information is |

| | | | |
|---|---|---|---|
| ● Types of Services Provided<br>● Notes<br>● Marital Status<br>● First Language<br>● Client Contact Information<br>● Residence Status<br>● Home Ownership<br>● Emergency Contact Information<br>● Health Insurance Type<br>● Primary Provider Indicator<br>● Self-Reported days of good mental/physical health<br>● Frequency of social support<br>● Employment Status<br>● Education Status<br>● Monthly Income, Expenses, Housing Expenses<br>● Total Savings<br>● Income Category | | | collected at intake, at discharge, and periodically throughout Care Coordination as major changes occur. |
| Goals/Family Success Plan/Client Interactions<br>● Reason for Referral<br>● Goal Development<br>● Goal Progress<br>● Client Strengths<br>● Client Struggles<br>● Culture Discovery<br>● Goal Notes<br>● Next Steps<br>● Interaction Date<br>● Interaction Goal<br>● Interaction Notes | ● Care Coordinators | ● System Administrators<br>● Care Coordinators | This data comprises the case management notes maintained by the Care Coordinator in the process of service delivery. It is utilized primarily for providing quality review of services provided. |

# Client Informed Consent

Prior to, or during the course of, the entry of any personally identifying information into CoactionNet by a Referral Network Partner or Care Coordinator, the individual recording data within CoactionNet must receive a consent form signed by the Client allowing *Driving the Dream*  to use and disclose this information in a manner that is consistent with this policy. Specifically, the Client will be asked to record consent for enrollment in Care Coordination with any Care Coordination Hub and for the provision of services related thereto. The Client will also be asked to record consent for each referral made through *Driving the Dream* on that Client's behalf.

## Data Use

Data collected by *Driving the Dream* will be used in accordance with the following policies:

- **Individually Identifiable Data** - will be made available to registered users of the CoactionNet system who are registered as a Referral Network Partner or Care Coordinator, consistent with access limits as described above. These registered users agree to maintain the strict confidentiality of any data entered into or obtained from the CoactionNet system. This information will be used only for legitimate client services and administration of the above named agency. Any breach of confidentiality will result in immediate termination of the user's CoactionNet account. Additionally, identified breaches of confidential information will initiate an ethics review of the user's employing agency in partnership with agency staff. The results of the ethics review will be made available to *Driving the Dream* and leadership of the employing agency.
- **Anonymized Individual Data** - will be made available to UWMS, *Driving the Dream* Network Partners, and contracted partners or vendors as deemed appropriate by *Driving the Dream* data management staff. Data will be anonymized by replacing the client's name with the client's record ID passed through a one-way hashing function (bcrypt), rounding the client's date of birth to the nearest month, removing the client's address (save for the zip code), and any other procedure which eliminates the possibility of identifying a specific client from provided data. This data will be provided for research purpose, and should in no way be used in an attempt to identify an individual client. Such a use will constitute a breach of this privacy policy and will result in loss of access to this data.
- **Aggregate Data** - will be made available to UWMS, *Driving the Dream* Network Partners, granting agencies, and the general public. This data will include no individual client information, and will reflect the status of the *Driving the Dream* service population as a whole. No aggregate data will be provided in which a subgroup of that data contains information regarding fewer than 15 Clients.

## Policy Violations

Any use, collection, or dissemination of Client data in a manner inconsistent with this policy will result in an impact analysis, ethics review, and notification of the appropriate party. In the case that data is released by or obtained from CoactionNet, through willing participation or criminal activity, in a manner inconsistent with this policy, UWMS and *Driving the Dream* will immediately notify CoactionNet of the incident (72 hours from discovery, maximum).

*Driving the Dream* staff will work with CoactionNet staff to conduct an impact assessment and prepare a remediation plan, which will include notification of the Referral Network Partner or Care Coordination Hub providing services to any Client affected by the exfiltration of data.

*Driving the Dream* staff will partner with the notified party to provide the impact assessment and to prepare a response, including but not limited to notification of affected Clients and Client education on potential impacts and personal mitigation procedures.

All *Driving the Dream* Referral Network Partners, Care Coordination Hubs, and other associated entities are required to report any suspected release of Client information to *Driving the Dream* staff in as expedient a manner as possible.

## Exceptional Circumstances

*Driving the Dream* complies with all relevant sections of the NASW Code of Ethics, including: “The general expectation that social workers will keep information confidential does not apply when disclosure is necessary to prevent serious, foreseeable, and imminent harm to a client or other identifiable person” (standard 1.07[c]).

In cases where there is ambiguity regarding the balance between Client confidentiality and safety, *Driving the Dream* and Network Partners will seek ethical and legal counsel prior to the use or release of any Client information in an effort to ensure Client safety.

No part of this privacy agreement is intended to replace or circumvent state, local, or federal laws, and compliance with this policy should not conflict with adherence to legal responsibility.

However, beyond the clear legal and professional ethical exceptions described herein, no exception to this policy is granted for individual moral, ethical, or religious reasons. Disclosure of confidential information on such grounds as suspected non-violent criminal behavior, suspected or confirmed substance abuse, suspected or confirmed non-legal immigration status, or any other non-excepted basis is considered a violation of this privacy policy and will be responded to as such.

# Appendix E

## Referral and Program Enrollment Consent Forms

# Driving the Dream Referral Form

## Client, April K

Quick View Information

## Referring Organization

## Consent

***Consent to Share Referring Information**

○ Hide Referring Organization Information
○ Share Referring Organization Information

I am consenting to allow agencies that are part of the DTD Network to share select pieces of information about me in order to provide high quality timely services. This information includes:

- My contact information
- Information I provided on the *Driving The Dream* referral form and/or intake form
- Assessments that would be helpful to other service providers so that I do not need to share the same information again
- DTD-related consent forms
- Results of referrals to service providers or meetings with my Care Coordinator

**Client Consent**

□ Client has agreed to consent over the telephone

**Client Signature**

**Name**

Full Name

**Signature**

## Contact Information

## Care Coordinator Referral and Appointment

CoactionNet

## *Driving the Dream*
## Information Release Consent Form

*Driving The Dream (DTD)*, a United Way of the Mid-South (UWMS) initiative, envisions a Mid-South in which all people have equitable access to the fundamental resources and supports needed to achieve their hopes and dreams. *DTD* enhances service providers' capacity to achieve this goal by improving communication and coordination of care between the various providers and systems involved (e.g., housing, education, healthcare, etc.). Achieving this objective will require coordination and collaboration between the UWMS and the *DTD* partners, including the sharing of client information and data.

### 1. Release of Information

I am consenting to allow agencies that are part of the *DTD Network* to share select pieces of information about me in order to provide high quality timely services. This information includes:

□ My contact information
□ Information I provided on the *Driving The Dream* pre-enrollment and/or intake form
□ Assessments that would be helpful to other service providers so that I do not need to share the same information again
□ DTD-related consent forms
□ Results of referrals to service providers or meetings with my Care Coordinator

### 2. Purpose and Use of Information

I understand that the purpose for accessing and sharing information or data is to better connect me to services and assess my progress toward reaching my goals. I understand that the information gathered may be used in the following ways:

1) To connect me to requested service providers and to provide service providers with an understanding of my situation and related needs
2) For evaluation, research, or quality improvement activities
3) Reports to program funders

If used in this way, my personal identifiable information would never be shared. No information or data will be used for any other purpose.

### 3. Your Rights

By signing below, you give written permission for UWMS and *DTD* partners to share your information or data with each other and with other appropriate service providers.

You have the right to revoke this authorization, in writing, at any time by sending an email to DTD@uwmidsouth.org. You will be made aware of all referrals, but if you have any questions please contact DTD@uwmidsouth.org.

I have read the above and give permission to UWMS and all *DTD* partners to have access to my information or data to be used solely for the purposes stated above.

| | |
|---|---|
| ______________________________<br>Printed name of participant | ______________________________<br>Signature of participant or parent, guardian, or authorized representative (when required) |

______________________________________ ______________________________________
Printed name of person administering consent Signature of person administering consent

______________________________________
Date

# CoactionNet
# Release of Information

I, ________________________________________________________________________, authorize
(Name of patient/client or their guardian)

____________________________________________________________________
(Name of program/agency making disclosure)

to disclose personal information collected regarding me (or my dependent as named below) in CoactionNet. CoactionNet is a database used to provide better coordination of services in our community. A list of participating CoactionNet agencies is attached. The most recent list of participating agencies can be accessed via CoactionNet.org.

The **purpose** of the disclosure authorized in this consent is to provide information within the CoactionNet system for the following reasons:

- Ensure participants receive timely and appropriate services
- Reduce the need for participants to repeat the same information with various agencies that can be of assistance in meeting service needs
- Provide oversight and meet reporting requirements
- Allow information to be collected to conduct program evaluation
- Use non-identifying data to compare participant information (service usage, outcomes, demographic information, etc.) with other aggregate community data

**Information shared** with this release of information with the partners on CoactionNet includes:

- Name
- Date of birth- if full or partial date is provided
- Demographic data- age, race, gender, ethnicity
- Social security number- if full number or last four digits were provided (only last four digits visible during database search)
- CoactionNet client identification number
- Nickname and/or alternate identification number(s), if applicable
- Enrollment status for program(s) listed above

CoactionNet system administrators provide technical support for agencies and individuals entering data into the system. System administrators have access to all information in the database for the sole purpose of ensuring the system is used according to privacy restrictions and that quality data is entered. System administrators adhere to strict confidentiality rules regarding personal information they encounter.

I understand that my client records are protected under state and federal regulations governing confidentiality of patient records. I further understand that the data will be shared electronically, the risks involved in online data collection and distribution, and authorize collection and distribution of personal data via electronic transmission. I understand further that:

- The regulations are the Federal Law of Confidentiality for Alcohol and Drug Abuse Patients, (42 CFR, Part 2) and the Health Insurance Portability and Accountability Act of 1996 (HIPPA), 45 CFR, Parts 160 & 164.
- The records cannot be shared without my written consent except as provided for in the regulations.
- I also understand that I may end this consent at any time.

# CoactionNet
# Release of Information

- I understand that there may have been information shared and services provided based on this consent when it was in effect. Ending this consent cannot change that.
- I understand that any notice to end this consent must be in writing.
- This consent will automatically expire: _______________ (one year from today)
- I understand that generally _____________________________________ (agency) may not condition services on whether I sign a consent form, but, in certain limited circumstances I may be denied treatment if I do not sign a consent form.

I understand that I may refuse to authorize information disclosure and that in certain limited circumstances I may be denied treatment or services if I decline to authorize disclosure of information necessary to determine eligibility status for this program.

I understand that by signing below, I give the agency listed above permission to provide services to the participant above identified below and to collect and report personal data as described in this authorization agreement.

| | |
|---|---|
| ________________________________________ | ________________________________________ |
| Printed name of participant | Signature of participant or parent, guardian, or authorized representative (when required) |

_______________________________________
Date

# CoactionNet
# Release of Information

Participating CoactionNet Agencies:*

901 BLOC Squad
Agencies Participating in Coordinated Response to Elder Abuse
Agape Child and Family Services
Aging Commission of the Mid-South
Ave Maria Home
Baptist Memorial Hospital
Cathedral of Faith
Community Legal Center
Exchange Club Family Center
Family Safety Center
Hickory Hill Community Redevelopment Corporation
Le Bonheur Children's Hospital
Mayor's Institute for Excellence in Government
Memphis Area Legal Services
Memphis Police Department
Meritan
Metropolitan Inter-Faith Association
Plough Foundation
Porter-Leath Children's Center
Rangeline Community Development Corporation
RISE Foundation
Shelby County Crime Victims Center
Shelby County District Attorney General
Shelby County Office of Early Childhood and Youth
South Memphis Alliance
University of Memphis
University of Tennessee

*The most recent list of participating agencies can be accessed via CoactionNet.org.