Florida Department of Children and Families

Substance Abuse and Mental Health

Financial and Services Accountability Management System (FASAMS)

Pamphlet 155-2 Chapter 2 Access Management

Last Revision Date: 03/28/2019

Version 13.0

Table of Contents

1 Introduction

This chapter provides general guidelines for ensuring the privacy and security of Protected Health Information (PHI) maintained in Financial and Services Accountability Management System (FASAMS) and other Substance Abuse and Mental Health (SAMH) systems. The purpose of this chapter is twofold:

- To highlight the basic privacy and security safeguards that must be followed by authorized persons when performing a function that involves the use or disclosure of Protected Health Information in SAMH systems; and
- To describe the procedures for requesting and obtaining access to SAMH systems, including the policy directive for compliance with security awareness training requirements.

1.1 Terms and Acronyms

The following table provides a list of business and technical acronyms/terms used in this document.

Acronym/Term	Definition
CFOP	Department of Children and Families Operating Procedure
CFR	Code of Federal Regulations
DCF	Department of Children and Families
FASAMS	Financial and Services Accountability Management System
HIPAA	of 1996 (HIPAA) is United States legislation that provides data privacy and security provisions for safeguarding medical information.
IRAS	Incident Reporting and Analysis System
LDAP	Lightweight Directory Access Protocol allows a user the opportunity to access many Department applications with a single user name and password.
OITS	Office of Information and Technology Services
ME	Managing Entity
PHI	Protected Health Information
SAMH	Substance Abuse and Mental Health
SAMHIS	Substance Abuse and Mental Health Information System
VPN	A virtual private network (VPN) extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. Applications running across the VPN may therefore benefit from the functionality, security, and management of the private network.

2 Protected Health Information (PHI)

The SAMH systems contain some of the 18 data elements contained in Title 45, Code of Federal Regulations (CFR), Parts 160 and 164, which is the Final Rule of the Health Insurance Portability and Accountability Act (HIPAA) establishing the national standards to protect individuals' medical records and other personal health information, including the privacy of individually identifiable health information. As such, only authorized persons, who must protect this individually identifiable information from accidental or intentional misuse, can access it.

The use or disclosure of any individually identifiable information in the SAMH systems must be in accordance with all federal and state laws and regulations, including guidelines and standards to guard data integrity, confidentiality, availability, and reliability. Those that apply directly or indirectly to the security and privacy of data in the SAMH systems include, but are not limited to, the following:

- Title 45 Code of Federal Regulations (CFR), Parts 160 and 164: Standards for Privacy of Individually Identifiable Health Information – Final Rule of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).
- Title 42 Code of Federal Regulations (CFR), Part 2: Confidentiality of Alcohol and Drug Abuse Patient Records.
- Section 394.4615, Florida Statutes: Confidentiality of Mental Health Clinical Records.
- Section 397.501(7), Florida Statutes: Right to Confidentiality of Substance Abuse Client Records.
- Section 916.107(8), Florida Statutes: Confidentiality of Clinical Records for Mentally Deficient and Mentally Ill Defendants.
- Title 45 Code of Federal Regulations (CFR), Part 142: Security and Electronic Signature Standards – Final Rule of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).
- Section 282.318, Florida Statutes: Security of Data and Information Technology.
- Department of Children and Families Operating Procedure (CFOP 50-2): Security of Data and Information Technology Resources.

3 Basic Security Safeguards

Below are the minimum-security measures to protect data in the SAMH systems from accidental or intentional unauthorized disclosure, modification, or destruction by persons within or outside of the department.

- Two layer authentication. Each user must authenticate with the DCF network through a VPN connection using an LDAP account issued and managed by DCF. Access to SAMH systems is provided through a site-to-site VPN connection that can only be accessed after authenticating with the DCF network.

- Individual User Account. Each user must have a unique user account. This account consists of the following information:
  1. A personal identifier (i.e., User Logon ID) that is assigned and controlled by the SAMH OITS Access Team
  2. A private password. The FASAMS system will allow the user to set up a private password during their initial login.
     a. For example, in FASAMS, the user will be prompted to change their password every 60 days. A password reset reminder will be sent via email 15 days prior to the password expiration.

- Each user account will be associated with a role. The role controls what functionality the user has access to. Refer to Appendix C of this document for a list of permissions associated with each role.

- A FASAMS user account can be associated with a group. The user will only have access to the data submitted by that group. For example, a user associated with ME 1 cannot see, access or update data from ME 2. In the event that a Provider has contracts with multiple managing entities, the user with ME 1 can only see data for that provider submitted under that ME.

- The online Security Awareness Training and the HIPAA Training **must** be taken annually. In addition, all DCF employees and employees of private and public agencies, who have access to departmental information shall comply with, and be provided a copy of CFOP 50-2, and shall sign the DCF Security Agreement form CF114 annually.

- Users are prohibited from sharing their passwords and User Logon IDs with other individuals. They are also prohibited from sharing or discussing client-identifying information (PHI) with anyone unless the other person is also an authorized user or the agency has identified the person as having a need to know in accordance with agency operating procedures.

Any computer, which contains or has access to SAMH data or other individually identifiable information**, must** be password protected and should be located in a secure area on a locked down floor. The computer should be programmed to time out or to turn off automatically after 15 minutes or less without activity, and the room **must** be locked when the user is not physically in the room.

- Screensavers must be used and be password protected.

- Any file containing confidential information that is not stored in a secure computer must be kept in a secure location whose accessibility requires the use of lock and key.

- SAMH data or other individually identifiable information should never be sent to a fax machine number or to a printer unless a user is absolutely sure that the recipient equipment is located in a secure location accessible only to authorized users.

- When sending client information by e-mail, it must be encrypted and password protected. A minimum of 128-byte encryption is required when using this process. Never send client data in the body of the message. Passwords should be encrypted and sent in a separate email.

- Users at all levels (state, circuit/region, ME and provider) should use preventive measures to minimize the risk of destruction, theft or loss of equipment and software, and to protect SAMH data from unauthorized disclosure, misuse, modification or destruction.

- Supervisors and Data Liaisons at all levels (state, circuit/region, ME and provider) are responsible for ensuring that users are trained and that appropriate access is allowed.

- FASAMS Account Access Parameters

  Fail Logon Limit: 5 times
  Duration of Failed Login Lockout: 15 minutes
  Password Expiration Days: 60 calendar days
  Password Minimum Length: 8 characters (at least 1 uppercase letter, 1 lowercase letter, 1 number and 1 special character)
  Password Minimum Age: 1 day (password can only be changed once per 24 hours)
  Previous Password Number: 10 (cannot reuse last 10 passwords)
  Account Lock: 45 calendar days of inactivity
  Account Disabled: 60 calendar days of inactivity

- Other SAMH Systems Account Access Parameters
  Fail Logon Limit: 3 times
  Duration of Failed Login Lockout: 15 minutes
  Contact your SAMH Access Administrator to unlock your account
  Password Expiration Days: 45 calendar days
  Password Minimum Length: 6 digits (numbers and/or letters)
  Password Maximum Length: 8 digits (numbers and/or letters)
  Previous Password Number: 15 (cannot use last 15 passwords)
  Account Lock: 45 calendar days of inactivity
  Account Disabled: 60 calendar days of inactivity

- DCF Supervisors must immediately notify the DCF Help Desk when a user has separated from DCF or no longer need SAMH system access in their current job duties. See Appendix B of this document.

- External Supervisors must immediately notify their SAMH Data Liaison when a user has separated from the organization or no longer needs SAMH system access in their current job duties. See Appendix B of this document.

- The SAMH Data Liaisons must immediately lock the account of any user who has separated from the organization or no longer needs SAMH system access in their current job duties, then notify the DCF Help Desk.

- The DCF Help Desk will send a ticket to the SAMH OITS Access Team to immediately disable the SAMH system account of users who no longer needs access due to separation or change in job duties.

- DCF has the right to audit any organization that has employees with access to SAMH systems.

4 Key Roles and Responsibilities for SAMH Access Management

Role	Responsibilities
User	• Completing Form CF114, SAMH Database Access Form and take the Security Awareness and HIPAA prior to requesting access to SAMH systems
Supervisors immediate DCF or External employee supervisors	• Ensuring that staff members complete Form CF114, SAMH Database Access Form and take the Security Awareness and HIPAA prior to requesting access to SAMH systems • Providing supervisor signature for CF114, and SAMH Data Base Access Form • Following the procedures described in Appendix A of this document for requesting access to SAMH systems • DCF Supervisors – Notifying the DCF Help Desk when a FASAMS user has separated from DCF or no longer need access to SAMH systems in their current job duties • External Supervisors – Notifying their SAMH Data Liaison when a user has separated from the organization or no longer needs access to SAMH systems in their current job duties

SAMH Data Liaison - include representatives Managing Entities, providers with direct contracts with DCF, state mental health treatment facilities, and any public or private agency that has access to SAMH systems	• Verifying that all required forms are received from the supervisor with appropriate signatures
	• Providing a Data Liaison signature for the SAMH Database Access Form
	• Ensuring that all appropriate staff members and staff members of their sub-contractors complete the Security Awareness and HIPAA training annually
	• Trainings must be completed annually within 45 days of training updates by DCF
	• Lock accounts for users who no longer need access to SAMH data
	• Ensuring a SAMH systems authorization process/policy is in place. The process must be auditable
	• Providing a copy of their SAMH systems authorization process/policy to DCF every 2 years
	• Following the procedures described in Appendix A of this document for requesting access to SAMH systems
	• Providing a list of current authorized signatories for the SAMH systems Database Access Forms to DCF
	• Maintaining physical or digital copies of all forms and certificates for audit purposes
	• Periodically reviewing their active user accounts in SAMH systems:
	  ○ Locking accounts that are no longer needed. See Appendix B of the document
	  ○ Ensuring that currently active accounts have the minimum access needed for their job

Role	Responsibilities
	• Providing DCF with a quarterly report that indicates when accounts were reviewed and the number of active accounts that were locked
SAMH Access Team – SAMH Program Office Staff	• Verifying that Form CF114, SAMH Database Access Form and the Certificates for Security Awareness and HIPAA have been received and appropriate forms signed by authorized Data Liaisons • Providing a SAMH Access Team signature for the SAMH Database Form • Ensuring the annual list Security Awareness and HIPAA recertification is sent to the Data • Maintaining physical or digital copies of all forms and certificates for audit purposes • Maintaining a list of authorized signatories for Data Liaisons
DCF Help Desk	• Providing a single point of contact for user to submit problems and/or issues • Accepting incidents from Users • Creating a FootPrints ticket with complete reported information at a sufficient level of detail • Providing the user with a FootPrints number for the reported incident • Answering user account issues, navigation questions and/or basic general functional questions • Resolving Tier 1 incidents using Knowledge Transcripts for known errors and knowledge topics • Notifying the User of Incident resolution and gaining approval for ticket closure • Escalating incidents for resolution outside of Tier 1 scope • Communicating the next steps to the user
Regional Security Team	• Ensuring LDAP accounts are created for new users who need access to SAMH systems • Suspending LDAP accounts for users who have been reported as separating from the organization or no longer needs access to SAMH systems in their current job duties
SAMH OITS Access Team – Office on Information Technology Systems staff	• Following the procedures described in Appendix A of this document for creating user accounts • Periodically reviewing active user accounts and (1) disabling accounts that are no longer needed, and (2) ensuring that currently active accounts have the minimum access needed for their job • Ensuring a SAMH systems authorization process/policy is in place for all SAMH systems users. The process must be auditable

5 Procedures for Requesting and Obtaining Access to SAMH Systems

Any person requesting access to FASAMS must complete, sign and submit the documents listed below.

- The DCF Access Authorization Request Form
  - DCF Employee - http://eww.dcf.state.fl.us/security/forms.shtml
  - All others - See your SAMH Data Liaison for the form
- The DCF Security Agreement Form (CF114), pages 1 and 2 only.
  - http://wwwre.myflfamilies.com/service-programs/substance-abuse/pamphlet-155-2-v12
- The SAMH systems Database Access Request Form
  - Same location as above
- The online Security Awareness Training Certificate
  - http://www.myflfamilies.com/general-information/dcf-training
- The online Health Insurance Portability and Accountability Act (HIPAA) Training Certificate
  - Same location as above

All documents listed above should be submitted according to the process shown in Appendix A of this document.

Once the approval and authentication process has completed, a DCF LDAP account (if needed) and a user account will be created. For external users, access to SAMH systems is through a VPN connection to the DCF network. The DCF LDAP user name and initial password for VPN installation will be emailed to the requestor by the SAMH Access Team.

FASAMS:
The user will receive an automated email from FASAMS which includes a link for FASAMS password creation. This emailed link is active for 12 hours only. Once the user completes the password setup, their account will be activated. The user must have a DCF LDAP account prior to creating a password for FASAMS.

All other SAMH Systems:
The SAMH Access Team will email the user's system username and a temporary password to the requestor. External users must have a DCF LDAP account prior to logging into the SAMH system and completing their password setup.

6 Troubleshooting

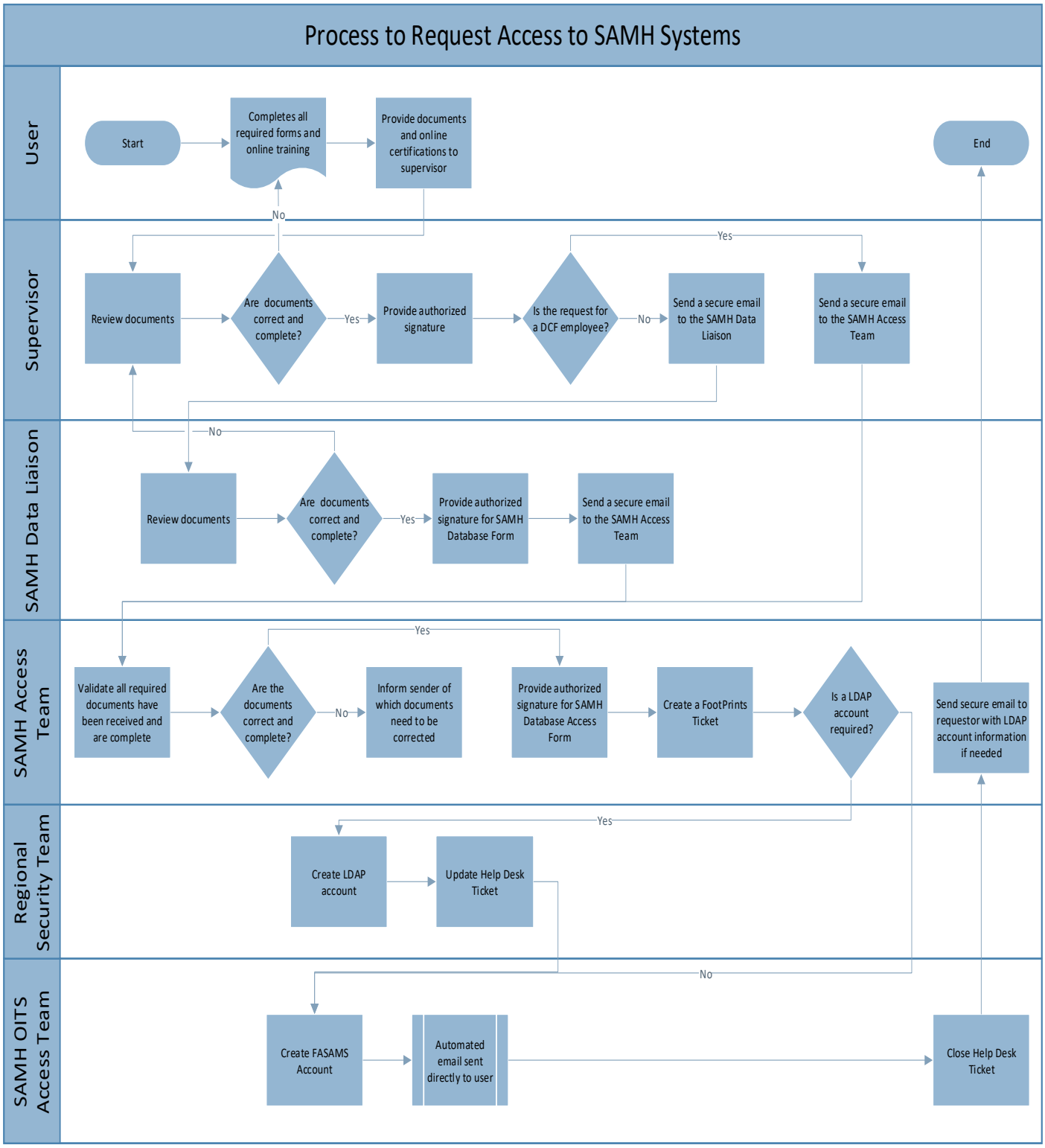
Problem	Solution
Error message received when attempting to confirm account creation from FASAMS email.	Contact the DCF Help Desk to reset if it has been more than 12 hours.
Error message received when attempting to confirm account creation from FASAMS email.	1. Verify that your VPN access has been setup and you are connected to the VPN. 2. If the issue persists, contact the DCF Help Desk.

Problem	Solution
Unable to log into SAMH systems.	1. Verify that your VPN access has been setup and you are connected to the VPN. 2. If the issue persists, contact the DCF Help Desk.
Forgot Username or Password for FASAMS	1. Use the "Forgot username or password?" 2. If necessary, contact the DCF Help Desk.
Forgot Username or Password for other SAMH systems	Contact your SAMH Data Liaison.
User account is locked.	1. For FASAMS: contact DCF Help Desk to reset. 2. For all other SAMHIS Databases: contact supervisor or SAMH Data Liaison
User account is disabled.	See your supervisor or SAMH Data Liaison to fill out the appropriate paperwork.
LDAP password will expire or has expired	1. Self Service: https://ad7lpx2m4rsete.dcf.state.fl.us/webapp/login.aspx 2. Contact the DCF Help Desk
FASAMS Password reset email expired.	Contact the DCF Help Desk to reset if it has been more than 12 hours.
I am a new user and need a user account.	See your supervisor or SAMH Data Liaison to fill out the appropriate paperwork.
Unable to connect to VPN	Contact the DCF Help Desk
Unable to connect to Internet	Contact your supervisor
Cannot view specific screen or save incident in SAMHIS/IRAS	Be sure 'state.fl.us' has been added to the Compatibility View Settings under Tools or the gear icon in command bar above application in Internet Explorer.

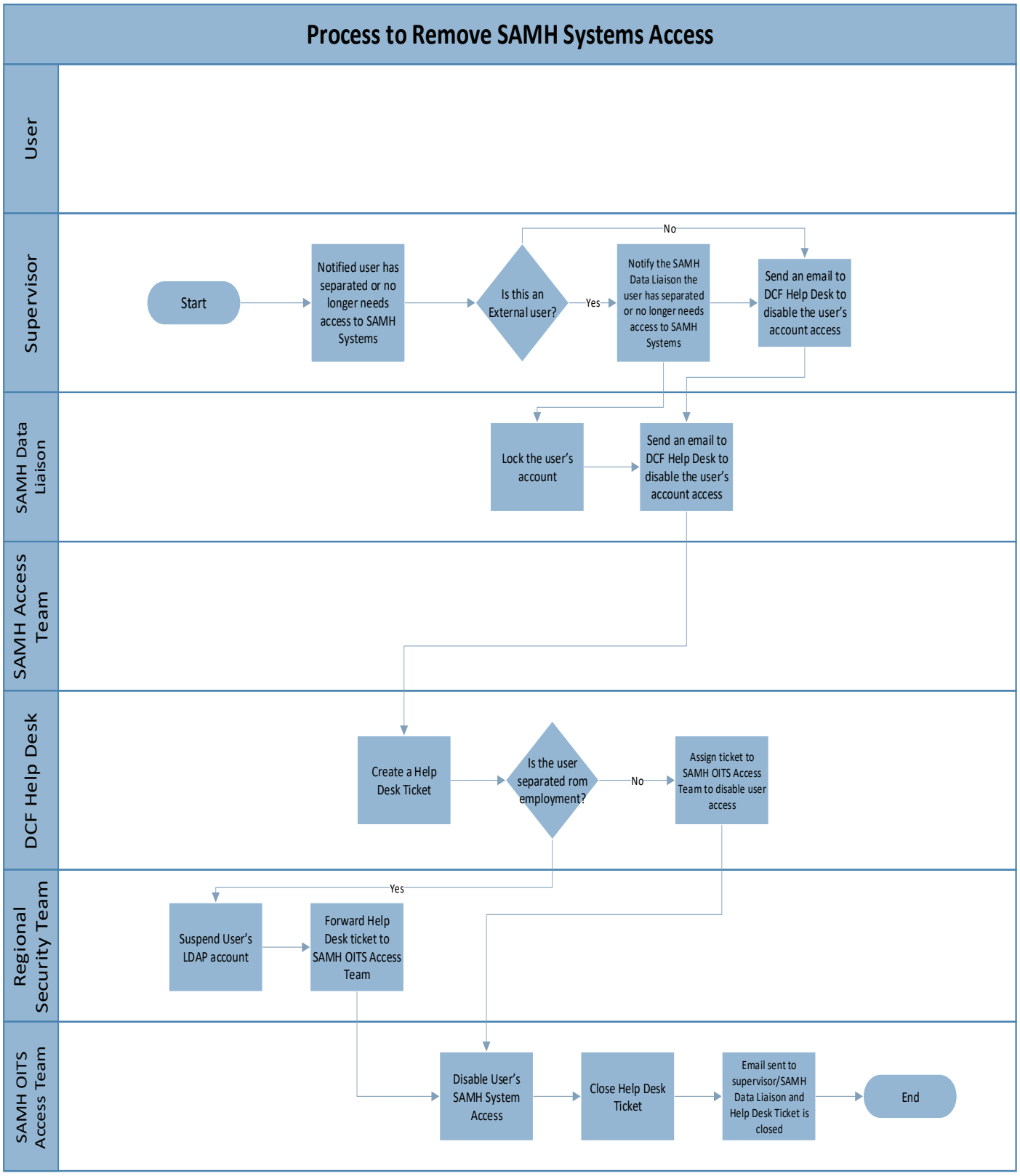
7 Contact Information

Who	Contact Information
DCF Help Desk	Phone: (850) 487-9400 or (855) 283-5137 (Toll-free) or Email: DCF.HELPDESK@myflfamilies.com FootPrints (DCF employee): **Self Service Portal (Footprints)**
SAMH Access Team	HQW.SAMH.AccessControlTeam@myflfamilies.com
SAMH Data Liaison	See your supervisor for your agency's liaison

8 Appendix A – Process to Request Access to SAMH Systems



9 Appendix B – Process to Remove SAMH Systems Access



10 Appendix C –SAMH Access Roles

FASAMS								
Permission	**DCF Administrator**	**Regional Office Administrator**	**Submitting Entity Administrator**	**Regional Office Staff User**	**Submitting Entity User**	**Financial Regional User**	**FSFN User**	**User Account Administrator**
Subscribe to Administrative Notifications	✓		✓					✓
Access All User Accounts	✓							✓
Can Grant Administrative Roles	✓							✓
Lock/Unlock User Accounts	✓	✓						✓
View Users	✓	✓	✓	✓	✓			✓
Edit Users	✓	✓	✓		✓			
Edit User Notifications	✓							✓
Reset User Password	✓	✓						✓
Assign All Groups	✓							✓
View Groups	✓		✓					✓
Edit Groups	✓							✓
View Roles	✓		✓					✓
Edit Roles	✓							
Access All Submitting Entities	✓							✓
View Submitting Entity	✓	✓	✓					✓
Edit Submitting Entity	✓	✓	✓		✓			✓
Access All Vocabulary	✓							
View Vocabulary	✓	✓	✓					
Edit Vocabulary	✓		✓					
View Business Rules	✓		✓					
Edit Business Rules	✓		✓					
Enable/Disable Rules	✓							✓
View Jobs	✓	✓	✓		✓			
View Job Submission	✓		✓					

FASAMS								
Permission	**DCF Administrator**	**Regional Office Administrator**	**Submitting Entity Administrator**	**Regional Office Staff User**	**Submitting Entity User**	**Financial Regional User**	**FSFN User**	**User Account Administrator**
Performance Reports								
Upload Job Submission	✓	✓	✓		✓			
Access SSRS	✓	✓	✓	✓		✓		
View Reports	✓		✓			✓		
View Financial Reports	✓					✓		
View Acute Care Reports	✓							
View Contract Compliance Reports	✓							
Edit Dynamic Data Sets	✓							
View Dynamic Data Sets	✓							
Unfinalize Dynamic Data Sets	✓							
View FSFN Extract	✓						✓	
View TEDS Extract	✓							
View Federal Reports	✓							
View TEDS Extract	✓							
View SHR Extract	✓							
View BCI Extract	✓							

SAMHIS, TANF, SANDR, DOC, and IRAS					
Permission	**DCF Administrator**	**Regional Office Administrator**	**Submitting Entity Administrator**	**Submitting Entity User**	**Regional Office Staff User**
SAMHIS and SANDR					
State Administrator	✓	✓	✓	✓	✓
Regional Administrator		✓	✓	✓	✓
Provider Administrator			✓	✓	
Provider Staff				✓	✓
Sub-Contractor				✓	
IRAS					
Incident Coordinator	✓	✓	✓	✓	✓
Viewer	✓	✓	✓	✓	✓
TANF					
TANF State Administrator	✓	✓	✓	✓	✓
TANF Regional/Circuit Administrator		✓	✓	✓	✓
TANF Provider	✓			✓	✓
TANF Sub-Contractor	✓			✓	
DC					
DC Administrator	✓		✓		

Regional Office Administrators will only have access to users and submitting entities within their assigned region.

Submitting Entity Administrators will only have access to users within their entity.