St. Clair County Community Mental Health

Confidentiality and Data Security Agreement

St. Clair County Community Mental Health (SCCCMH) has both a legal and ethical responsibility to safeguard the confidentiality and security of the information it manages, including the protected health information (PHI) of individuals it serves (*"recipients"*), as well as operational, proprietary, and employee data. This information may include, but is not limited to: its human resources data (such as personal employee information and records), payroll data, financial reports, research, internal reporting, strategic planning information, credentialing data, intellectual property, and data containing Social Security numbers, health insurance claim numbers, passwords, PINs, encryption keys, credit card numbers, or any other financial account information. Collectively throughout this agreement, these types of information, along with recipients' PHI, will be referred to as "**Confidential Information**".

In the course of my role with SCCCMH, whether as a direct employee or through a contracted agency, I understand that I may access or come into possession of these types of Confidential Information. I understand that I must only access and use this information when necessary to perform my job duties in accordance with SCCCMH's privacy and security policies. These policies can be found on SCCCMH's Policy Index internally via ADP or online at www.scccmh.org.

I understand that, in order to access Confidential Information and SCCCMH's systems (such as OASIS), or to provide services at any SCCCMH facilities, I must sign this Agreement and comply with its terms.

General Rules

1. I will act in the best interest of SCCCMH and in accordance with its Code of Conduct throughout my relationship with SCCCMH.
2. I understand that I should have no expectation of privacy when using SCCCMH information systems. SCCCMH has the right to log, access, review, and otherwise monitor information stored on or transmitted through its systems, including email, for system management and security enforcement purposes.
3. I understand that violation of this Agreement may result in disciplinary action, up to and including termination of employment, suspension, and loss of privileges. Additionally, it may lead to termination of authorization to work within SCCCMH's Contract System, in accordance with SCCCMH's policies, as well as potential civil and criminal legal penalties, as applicable for my role as an employee, volunteer, or contractor providing services.

Protecting Confidential Information

4. I will not disclose, discuss, or share any Confidential Information with others, including friends or family, unless they have a legitimate need to know for the performance of their SCCCMH job duties.
5. I will not take any media or documents containing Confidential Information home or to non-work locations unless explicitly authorized to do so as part of my job responsibilities.
6. I will not publish, disclose, or share any Confidential Information through personal email, through social media, or other internet sites unless explicitly authorized to do so in support of SCCCMH business and within scope of applicable regulations (e.g., HIPAA) and SCCCMH policies.
7. I will not misuse Confidential Information, nor will I divulge, copy, release, alter, or destroy Confidential Information except as properly authorized. I will only handle media and records in accordance with SCCCMH's Information Security Standards and Record Retention Policy (#03-002-0060).
8. When communicating health information verbally as a part of service delivery, I will take reasonable steps to prevent unauthorized disclosure, such as speaking in private areas or lowering my voice when appropriate.
9. I will not transmit, request, modify, or delete Confidential Information unless explicitly authorized to do so. I will ensure any external transmission of Confidential Information outside of the SCCCMH network including via email or other electronic communication methods, is encrypted in compliance with SCCCMH's Information Security Standards.

Following Appropriate Access

10. I will access only those systems, devices, and recipient records for which I have been officially authorized, and will do so exclusively through agency-approved devices. For contracted agencies, this includes using devices provided to staff by their respective organizations. Accessing such information on non-approved devices is prohibited and may result in disciplinary action.
11. I will access SCCCMH information, systems, or recipient records only when I have a legitimate business need and the necessary consent. Each time I access such information, I affirm that these conditions have been met, and SCCCMH may rely on that affirmation in granting access to me.

Using Mobile Devices, Portable Devices, and Removable Media

12. I will not copy or store Confidential Information on mobile devices, portable devices, Cloud storage (e.g., Google Drive, Microsoft iCloud), or removable media (e.g., laptops, USB Drives, smartphones) unless it is specifically required for my job duties. If storage of Confidential Information on removable media is necessary, I will ensure the information is encrypted according to SCCCMH's Information Security Standards.
13. I understand that any mobile device that synchronizes SCCCMH's data (e.g., SCCCMH email) may contain Confidential Information and as a result, must be secured with a password as required by SCCCMH Information Security Standards.

Doing My Part - Personal Security

14. I understand that my personal data will be tracked and used to monitor my access and use of Confidential Information.
15. I will:
    a. Use only my officially assigned User ID and password, and authentication token/app.
    b. Use only approved and licensed software.
    c. Use devices equipped with up-to-date virus protection software.
16. I will never:
    a. Share my passwords, PINs, or access codes.
    b. Allow another individual to use my digital credentials (e.g., User ID and password) to log into a computer system or to access, modify, or delete data.
    c. Use unauthorized tools or techniques to bypass or exploit security measures.
    d. Connect unauthorized devices or systems to the SCCCMH network.
    e. Use non-approved devices to access SCCCMH systems, including OASIS (Electronic Health Record software).
17. I will practice secure workstation practices such as keeping Confidential Information out of sight when not in use, locking my screen when unattended, and positioning screens to prevent public viewing.
18. I will immediately notify my Supervisor, the Corporate Compliance/Privacy Officer, or the Security Officer in the event of:
    a. Suspected or actual disclosure or compromise of my password;
    b. Loss or theft of media with Confidential Information stored on it;
    c. Any signs of a virus or malware infection on any system;
    d. Any activity that violates this Agreement or SCCCMH's privacy and security policies; or
    e. Any other incident that could potentially impact the security of SCCCMH systems.

Upon Exit from the Organization

19. I acknowledge that my responsibilities under this Agreement will remain in effect even after my employment, contract, or affiliation with SCCCMH ends.
20. Upon the end of my relationship with SCCCMH, I will immediately return any documents, devices, or media containing Confidential Information to SCCCMH.
21. I understand that I do not hold any ownership rights to any Confidential Information accessed or created by me during and in the scope of my relationship with SCCCMH.

By signing this document, I acknowledge that I have read this Agreement in its entirety and I agree to comply with all of the terms and conditions stated above.

Signature	Date
Print Name	Supervisor's Name
Name of Company, Business, or Employer (if applicable)	