Missouri Department of MENTAL HEALTH

Social Security Administration Training

Requirements and Procedures for the Exchange of Electronic Information with the Social Security Administration (SSA)

Holly Hern, DMH Chief Security Officer

Michael Held, DMH Assistant General Counsel/HIPAA Privacy Officer

Created March 2017

(Revised September 2025)

Social Security Administration Federal Standards

- The SSA is required by law to oversight of the protected information it provides to the Department of Mental Health (DMH) and is utilized by department employees and contractors.
- All DMH employees, contractors, and agents who access SSA-provided information must be trained as to the sensitivity and protection of SSA-provided information.
- DMH employees, contractors, and agents are subject to and must comply with the Privacy Act of 1974, the Federal Information Security Management Act (FISMA) and relevant policy issued by the National Institute of Standards and Technology (NIST) when accessing or using SSA-provided information.

What is protected SSA-Provided Information?

The Electronic Information Exchange (EIE) is an electronic process in which PII under SSA control is disclosed to a third party. DMH uses SSA-provided information to verify and add client information in CIMOR and ultimately in CHARTe and ConneXion.

The information includes personally identifiable information (PII) defined as information which used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with another personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

Safeguard of SSA-Provided Information

All DMH employees, contractors, and agents agree to:

- Protect SSA-provided information with efficient and effective security controls.
- Only use SSA-provided information for a legitimate work purpose. Viewing and copying of SSA-provided information for a non-work purpose is prohibited.
- SSA-provided information shall be disposed of properly and timely when no longer needed.
- Report a breach or loss of SSA-provided data immediately to a local DMH Privacy Officer.
- Follow procedures to protect the network from malware attacks, spoofing, phishing and pharming, and network fraud prevention.

Misuse of SSA-provided information may lead to criminal, administrative, and civil sanctions, contract termination, and/or employee discipline.

CIMOR, CHARTe and ConneXion Access

By accessing CIMOR, CHARTe or ConneXion, DMH employees, contractors, and agents are acknowledging that they will abide by, not only the DMH department operating regulations (DORs), but all relevant federal laws, restrictions on access, use, disclosure, and the security requirements contained within the department's agreement with SSA.

A copy of the SSA agreement and related documents are available on the DMH portal for review.