# Michigan Center for Effective IT Adoption

# Security Risk Analysis Report

*for*

## Sanilac County Community Mental Health

M-CEITA | Michigan Center for Effective IT Adoption

May 25, 2017

## Previous SRA Date(s):

| |
|---|
| 5/17/2016 |
| 6/26/2015 |
| |
| |
| |
| |
| |
| |
| |

## Contents

## Executive Summary

The following is a report of the Security Risk Analysis (SRA) that was performed at Sanilac County Community Mental Health on May 25, 2017. The objective of the SRA is to facilitate your compliance with Objective 1 of the Meaningful Use requirements.

Under the Meaningful Use requirements of the EHR Incentive program, Objective 1 mandates the protection of electronic Protected Health Information (ePHI) that is created or maintained through your certified EHR system. Accordingly, the core measure requires the performance of a security risk analysis to identify and mitigate security deficiencies within your risk management process, based on the HIPAA standards specified at 45 CFR 164.308(a)(1), 45 CFR 164.306(d)(3), and 45 CFR 164.312(a)(2)(iv).

Given the limited scope of this Security Risk Analysis, your compliance with Objective 1 does not mean full compliance with all HIPAA Privacy and Security requirements. Additional actions beyond the limits of the SRA are required of you for conformity with broader HIPAA regulations.

Sanilac County Community Mental Health is responsible for the validity of the responses provided in the SRA. M-CEITA's role in the SRA is limited to supporting clients by providing guidance in completing the questionnaire, recommending corrective actions and providing sample materials for policy-related remedial actions. Sanilac County Community Mental Health is also responsible for implementing the recommended corrective actions in order to substantiate positive attestation to fulfilling Objective 1.

Results from the assessment indicate a total of 2 risk exposures. These require the application of administrative and technical control measures to safeguard the privacy and security of ePHI at Sanilac County Community Mental Health.

To facilitate your compliance, a Corrective Action Plan is enclosed along with other resources with which you can mitigate your risk exposures. Please note that the results of the SRA activity are not exhaustive of other potential risks inherent in the operation of Sanilac County Community Mental Health's business activities. You are therefore encouraged to leverage resources available to your organization to ensure a comprehensive compliance with HIPAA and HITECH Privacy and Security requirements.

# 1. Introduction

## 1.1 Purpose

The purpose of this security risk analysis is to evaluate the adequacy of measures applied to assure the security and privacy of electronic Protected Health Information (ePHI) created or maintained through the Electronic Health Records system in use at Sanilac County Community Mental Health. Currently, this system is PCE. This risk analysis also examines other assets, processes, and resources that come in contact with ePHI, and essentially provides a structured qualitative assessment of the security of your operating environment. It addresses sensitivity, threats, vulnerabilities, risks and safeguards. Finally, the assessment recommends corrective measures to mitigate threats and associated exploitable vulnerabilities, all of which are required to be applied in order to substantiate your positive attestation to fulfilling the requirements of Objective 1.

## 1.2 Scope

The scope of this Security Risk Analysis is limited to assessing Sanilac County Community Mental Health's use of resources and controls (implemented or planned) to eliminate and/or manage vulnerabilities exploitable by threats internal and external to your organization. To that end, M-CEITA is providing this report and recommends appropriate remedial actions to correct identified lapses.

If exploited, these vulnerabilities could result in the:

- Unauthorized disclosure of data
- Violation of Patients' Privacy and Trust
- Unauthorized modification to the system, its data, or both
- Permanent loss or corruption of data
- Temporary loss or corruption of data
- Denial of service, access to data, or both to authorized users
- Loss of revenue
- Loss of physical assets

This Security Risk Analysis Report evaluates the **confidentiality** (protection from unauthorized access to systems or disclosure of data), **integrity** (protection from improper modification of information), and **availability** (continuous availability) of ePHI. Recommended security safeguards will enable management to make decisions about security-related initiatives.

## 2. Security Risk Analysis Approach

This security risk analysis methodology conforms to the guidelines in the National Institute of Standards and Technology's (NIST) Special Publication (SP) 800-30, *Risk Management Guide for Information Technology Systems* and *SP 800-66, Risk Guidance*. The assessment is limited in scope and evaluates security vulnerabilities affecting confidentiality, integrity, and availability of ePHI. The methodology addresses the following types of controls:

- **Management/Administrative Controls:** Management of the information technology (IT) security system and the management and acceptance of risks through appropriate policies and procedures.
- **Operational and Physical Controls:** Security methods focusing on mechanisms implemented and executed primarily by people (as opposed to systems), including all aspects of physical security, media safeguards, and inventory controls.
- **Technical Controls:** Hardware and software controls providing automated protection to the system or applications (Technical controls operate within the technical system and applications).

### 2.1 Asset Identification

The SRA started with the identification of your assets. Refer to the 'Practice Summary' and 'Inventory Preparation' tabs of your SRA Questionnaire.

### 2.2 Vulnerability and Threat Identification

The vulnerabilities and threats associated with your organization's assets were identified using NIST SP 800-66 and SP 800-30 guidelines. Vulnerabilities arise from flaws or weaknesses in your operating environment, while threats are potential means of exploiting these vulnerabilities.

### 2.3 Identify Current Security Risk Control Measures

The SRA exercise also examined your current security risk controls measures in order to identify potential gaps. These controls are comprised of administrative (e.g. policies and procedures), physical (e.g. secure areas and entry access controls), and technical (e.g. encryption, role-based access control, system activity logs) safeguards.

### 2.4 Determine the Likelihood and Impact of Adverse Events

In determining the likelihood of occurrence and the potential impact to the business activities of your practice by the exercise of any of the identified vulnerabilities and threats, the existence and effectiveness of control measures, as well as environmental factors were considered.

### 2.5 Establish the Level of Risk

The level of risk is a function of the existence and effectiveness of control measures, the likelihood of occurrence, and the potential impact on your business activities.

### 2.6 Recommend Corrective Actions

Having performed the foregoing actions, the next step is to recommend corrective actions to address the gaps. The Corrective Action Plan attached to this report contains these recommendations.

## 3. Findings and Recommendations

### 3.1 Findings

The results of the assessment indicate a total of 2 risk exposures in the following 2 areas:

1. Physical Security
2. Network Security

Details of these risk exposures are outlined in the Corrective Action Plan that is attached to this report.

### 3.2 Recommendations

For every item identified in the security risk analysis, the Corrective Action Plan outlines the recommended control measures, the resource(s) required for the corrective action and indicates the compliance guidance (i.e. whether the control measure is required or discretionary). These remedial actions consist of the development of policies and procedures, as well as applying appropriate technical control measures (such as the encryption) to safeguard protected health information.

## Conclusion

To facilitate your compliance with Objective 1, a Corrective Action Plan is enclosed along with other resources with which you can mitigate your risk exposures. These corrective actions need to be taken in order to substantiate an affirmative attestation to the 1st Objective of the Meaningful Use requirements. Should you need additional help, please contact your M-CEITA Representative.

## SRA Acknowledgement

The undersigned representative of Sanilac County Community Mental Health acknowledges as follows:

1. Sanilac County Community Mental Health is responsible for the validity of the responses provided in the Security Risk Analysis Questionnaire.

2. The role of the Michigan Center for Effective IT Adoption in the Security Risk Analysis process is limited to providing guidance in completing the SRA Questionnaire, as well as recommending corrective actions for any deficiency identified through the SRA.

3. Sanilac County Community Mental Health is also solely responsible for implementing corrective actions in order to validate positive attestation to fulfilling Objective 1 of the Meaningful Use requirements.

Date: _____ Name: _____

Signature: _____

*Please return a signed copy of this page to your M-CEITA Representative. Thank you.