St. Clair County Community Mental Health

Computer Acceptable Use Agreement

I have read, understand and agree to abide by the conditions stated in the St. Clair County Community Mental Health's Computer Information Systems Security administrative procedures (#08-001-0010). The St. Clair County Community Mental Health computer information systems are the property of St. Clair County Community Mental Health and subject to state and federal laws, rules and regulations. I will use the systems for performing authorized data exchange. I will not disclose my password or allow another person to log in with my User ID and password. I will access information on a need-to-know basis as required for official business related to my contracted tasks. I will not disclose any confidential, restricted or sensitive data to unauthorized persons. I will securely maintain any information downloaded, printed or removed in any format from the systems. I am giving expressed consent to St. Clair County Community Mental Health to monitor my activity on the systems. I will notify St. Clair County Community Mental Health regarding any change to the vendor task list which may require a change to accessing the information systems.

Vendor Name: _____

Vendor Email Address: _____

Vendor Phone Number: _____

Vendor Company: _____

Vendor Task List: _____

_____

CMH Equipment Assigned to Vendor: _____

_____

My signature below indicates that I have read and understand this document, including the sections on HIPAA and the HITECH Act and the St. Clair County Community Mental Health's Information Systems Policies.

_____ _____

Vendor Signature: Date:

As responsible party for the vendor, my signature indicates that I have read, understood and verify this document, including the sections on HIPAA and the HITECH Act and the St. Clair County Community Mental Health's Information Systems Policies/ administrative procedures. I will notify St. Clair County Community Mental Health regarding change of the task list of this vendor, including termination, which requires a change to accessing the information systems.

Vendor Name: _____

(Vendor Supervisor Name)

Vendor Signature: _____ _____

(Supervisor Signature) Date:

St. Clair County Community Mental Health Approval:

☐ Approved ☐ Disapprove

_____ _____

Signature: Date:

HIPAA

The HIPAA Security Rule requires Covered Entities to implement a "Unique User Identification" standard for electronic systems with protected health information (ePHI). Unique user identification is a unique name or number used to identify and track specific individuals using ePHI systems, also referred to as "LOGIN ID" or "USER ID". This provides a means to verify the identity of the person using the systems. The User ID should only be used by the intended person; use by someone other than the intended person is a violation of the HIPAA Security Rule and fraud. Licensed health professionals who share their password may also be in civil and criminal violation of licensure law.

For more details see HIPAA Security Rule section 164.312 (Technical Safeguards).

The HITECH Act

The HITECH Act imposes data breach* notification requirements for unauthorized uses and disclosures of "unsecured PHI (protected health information) (basically "unencrypted PHI)", and business associates are also required to comply. Business associates are required to report security breaches to covered entities consistent with requirements, and area also subject to civil and criminal penalties under HIPAA if certain conditions exist. Civil penalties for willful neglect are increased under HITECH: up to $250,000 with repeat / uncorrected violations extending up to $1.5 million.

The Act requires that patients be notified of any unsecured breach and their PHI might have been accessed, acquired or disclosed as a result of that breach. If a breach impacts 500 patients or more then Health & Human Services (HHS) must be notified and also prominent media outlets of the geographic area will need to be notified. A business associate of a covered entity shall notify the covered entity of a breach, including identification of each individual whose PHI has been breached. A breach is considered discovered on the first day that any employee, officer or agent of an entity or associate becomes aware that a beach has occurred.

All required notifications must be made within 60 calendar days of the discovery of the breach. Burden of proof of all notifications falls on the entity or associate. Written notification to individuals (or guardian or next of kin) by first class mail to the last known address is required. If contact information is insufficient or out of date, a conspicuous notice can be provided on the entity's web page or a notice can be placed in print or broadcast media including a toll-free phone number to call for more information. If notification is urgent, a telephone call can also be used in conjunction with other forms of notification.

Notice of breach shall include:

1. A brief description including the date of the breach and the date of discovery, if known
2. A description of the types of PHI included in the breach
3. Steps the individual should take to protect themselves from harm from the breach
4. A brief description of how covered the entity is investigating, mitigating and protecting against future breaches
5. A toll free number, email address, web site, or postal address to contact for more information

*The term "breach" means the unauthorized acquisition, access, use, or disclosure of PHI which compromises the security or privacy of such information, except where an authorized person to whom such information is disclosed would not reasonably have been able to retain such information.

Read section 13402 of the HITECH Act for full details about breach notification.