

WCHO	<i>Policy and Procedure</i>		
Department HIPPA	# of Pages: 9		
Policy Name SECURITY OF CONSUMER RELATED INFORMATION	Type of Policy: <input type="checkbox"/> WCHO <input type="checkbox"/> Regional <input checked="" type="checkbox"/> Network		
Policy Number 13.007	Effective Date	Revision Date	Approval Date 10/21/04
Administrative/Board of Directors Sign Off			
Administrative Signature:			Date:
Board of Directors Signature:			Date:

In Conjunction with
Washtenaw County Community Support and Treatment Services

I. PURPOSE

To establish a system for insuring the security, privacy, integrity and confidentiality of all consumer related information.

II. APPLICATION

This policy applies to all Washtenaw Community Health Organization officials, employees, students and volunteers and those of organizations under contract with WCHO. Due to the unique nature of the collaboration between WCHO and CSTS, including integrated elements of the data systems, WCHO and CSTS shall coordinate efforts. External application of standards shall be defined in Chain of Trust Agreements and/or contract language.

III. DEFINITIONS

Access: The ability to use a computer system or physically secure a copy of the Clinical Records. More specifically in regard to electronic medical records, the ability to inspect, review, retrieve, store, communicate with, or make use of health information system resources or consumer identifiable data or both.

Access control: The prevention of unauthorized use of a computer system or a hard copy of the Clinical Record. Access control includes both prevention of unauthorized users and unauthorized uses by authorized users.

Authorization: Permission to access a computer system or a hard copy of the Clinical Record.

Healthcare Information: Any information, whether oral or recorded in any form or medium that: (a) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and that (b) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present or future payment for the provision of health care to an individual.

Personally identifiable health information: Health information that contains the consumer's identification (name, Social Security number, and so forth) or a sufficient amount of other information to allow identification of the consumer.

Personnel security: The components of a security system to ensure that (1) only reliable persons have access to information being protected, (2) they are trained in security and (3) they face discipline for breaches of security.

Physical access: The ability to interact directly with a computer system, such as by having a keyboard to enter or secure information or the ability to secure a copy of the hard copy clinical record.

Physical security: The components of a system that prevent unauthorized availability to computerized or hard copy clinical records.

Risk Assessment or Risk Analysis: The process of selecting appropriate measures to protect against particular dangers to computer systems, data and clinical records.

System security: The components of a security program that integrate physical and personnel security with procedures designed to protect health care information.

IV. POLICY

- A. It is the policy of WCHO and CSTS to ensure the security, privacy, integrity and confidentiality of all consumer related information in accordance with professional ethics and legal requirements.
- B. The responsibility for the security of health related information shall be assigned to a joint Security Committee appointed by the Washtenaw County Administrator and the WCHO Executive Director. The membership of this committee is further defined in Section VI of this policy. The County Administrator and the WCHO Executive Director shall jointly appoint a member of the Security Committee to act as Security Officer. The Security Officer shall be assisted by technical, program and administrative members of the committee.
- C. The Security Committee shall provide oversight to ensure that all employees, students, volunteers and contractors of WCHO and CSTS preserve the security, privacy, integrity and confidentiality of all information gathered in the course of providing mental health, substance abuse or health related services. The Security Committee shall ensure that WCHO, CSTS and their respective officers, employees and agents have the necessary

information to protect the security, privacy and confidentiality of personally identifiable health information to the highest degree so that consumers have confidence when providing information to WCHO and CSTS.

- D. The Security Committee is responsible for the development, coordination and oversight of security management systems that include:
- Risk analysis
 - Risk management
 - Corrective action
 - Applicable policies, procedures and standards
 - Security training and education
- E. The Committee shall also ensure that appropriate sanctions are in place for violations of standards and regulations. This shall include creating, administering and overseeing policies to ensure the prevention, detection, containment and correction of security/confidentiality breaches.

V. EXHIBITS

None

VI. REFERENCES

- A. Media Contact 01.020
- B. Utilization Management Policy 02.020
- C. Policy Statement on Email Use 02.040
- D. Program Outcome Assessment and Measurement 04.030
- E. Research 04.040
- F. Policy on Sentinel Events Reporting 04/050
- G. Facility Opening and Closing 06/130
- H. Keys 06.140
- I. Clerical Services 07.020
- J. Clinical Record Forms Procedures 8/040
- K. Closed Clinical Records Storage 8.050
- L. HSIS Confidentiality and Security 08/70
- M. Ethical Guidelines 05.100
- N. Emergency Management Plan 06.050
- O. Safety Management Program 06.060
- P. Referrals: External
- Q. Bill of Rights and Responsibilities 13.040
- R. Confidentiality and Access to Clinical Records 13.050
- S. Consent to Treatment Services 13.060
- T. Report and Review of Deaths 13.120
- U. Right to be Treated with Dignity and Respect 13.130

WASHTENAW COUNTY

- A. Emergency Procedures I.E2.1
- B. Emergency Management I.E3.1
- C. Internet and Email Policy I.15.3
- D. Mail and Courier Services I.M1.2
- E. Desktop Computer Purchases I.P7.1
- F. Risk Management Program Policy I/R6/1
- G. Automation and Telecommunications Us and Acquisition Policies
- H. Automation Use and Acquisition Procedures 3.1.1.3
- I. Policy to Limit Washtenaw County's Vulnerability Due to Automation Hardware and Software Use 3.1.3.1
- J. Network/Connectivity Strategy 3.1.4.1
- K. Systems Development and Life Cycle Procedure 3.1.5.3

VII. STANDARDS:

A. Privacy, Confidentiality and Accuracy of Information

The Security Committee shall ensure that comprehensive policies are in place that assure that officers, employees and contractors of WCHO and CSTS:

1. Maintain the security, privacy and confidentiality of consumer information in accordance with the Michigan Mental Health Code, the Michigan Public Health Code (for substance abuse regulations), the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and accreditation agency standards.
2. Collect and use individual health information on a need to know basis for the purposes of providing services and for supporting the delivery, payment, integrity and quality of those services.
3. Do not use or supply individual consumer information for non-health cares uses, such as direct marketing, employment or credit evaluation purposes.
4. Collect and use individual information only:
 - a. to provide proper diagnosis and treatment
 - b. with the individual's or authorized individual's knowledge and consent
 - c. to receive reimbursement for services provided
 - d. in the aggregate for research and similar purposes designed to improve the quality and to reduce the cost of care
 - e. in the aggregate as a basis for required reporting of health information
5. Recognize that information collected about and from consumers must be accurate, timely, complete, and available when needed:
 - a. ensuring the accuracy, timeliness and completeness of data
 - b. ensuring that authorized personnel can access information when needed

- c. completing and authenticating records in accordance with the law, professional ethics and accreditation standards
- d. maintaining records for the retention periods required by law and professional standards
- e. not altering or destroying an entry in a record, but rather designate it as an error while leaving the original entry intact and create and maintain a new entry showing the correct data. Updates and corrections will be noted and tracked historically.
- f. implementing reasonable measure to protect the integrity of all data maintained about consumers.
- g. following documented policies and procedures for the routine and nonroutine receipt, manipulation, storage, dissemination, transmission and/or disposal of consumer information.

6. Recognize that consumers have a right to privacy, and respect consumers' individual dignity at all times. Officers, employees, volunteers and contractors will respect consumers' right to privacy to the extent possible consistent with providing the highest quality care possible and with the efficient and safe administration of programs and services.

7. Act as responsible information stewards and treat all individual clinical record data and related financial, demographic and lifestyle information as sensitive and confidential. Consequently all officers, employees and contractors shall:

- a. treat all individual medical record data as confidential in accordance with professional ethics, accreditation standards, and legal requirements
- b. not divulge medical record data unless the consumer (or his or her authorized representative) has properly consented to the release or the release is otherwise required by law
- c. when releasing clinical record data, take the appropriate steps to prevent unauthorized re-disclosures, such as specifying that the recipient may not further disclose information without consumer consent or as authorized by law
- d. hold all subcontractors to the standards outlined herein
- e. release only the minimum amount of information necessary to meet the purpose of the disclosure and the scope of any release of information
- f. implement comprehensive measures to protect the confidentiality of medical and other information maintained about consumers
- g. remove consumer identifiers when appropriate, such as in statistical reporting and in research studies
- h. not disclose financial or other consumer information except as necessary for billing or other purposes authorized by law and professional standards

8. Report and respond to any actual or potential breach of security/confidentiality in accordance with reporting procedures.

9. Recognize that although WCHO holds the clinical record, the consumer has a right of access to information contained in the record and officers, employees and agents shall:

- a. permit consumers access to their clinical records in a manner consistent with the Michigan Mental Health Code and/or Public Health Code, and the Health Insurance

Portability and Accountability Act of 1996 (HIPAA), and any other applicable laws, rules, or regulations.

b. provide consumers an opportunity to request a correction of inaccurate data in their records in accordance with the law and professional standards. Corrections may consist of either an update to the record by professional staff or inclusion of a written statement by the consumer in the record.

10. Conduct appropriate employee orientation, training and termination procedures

11. All officers, employees, volunteers and contractors of WCHO and CSTS must adhere to this policy and all policies related to the security of consumer related information. Neither WCHO nor CSTS will tolerate violations of policies protecting consumer related information. Violation of policy is grounds for disciplinary actions, up to and including termination of employment and criminal or professional sanctions in accordance with Human Resources policies and Bargaining Agreements and federal sanctions under HIPAA.

B. Security Measures

The Security Committee shall also ensure that comprehensive plans are in place to address physical security, personnel security and systems security.

1. Physical security measures shall include physical access controls which limit physical access to program sites and consumer information, while ensuring properly authorized access. Features shall include but not be limited to: equipment and media controls, site security plans for all sites where consumer information is maintained, security of workstation locations, authorization procedures, maintenance procedures and records, need-to-know procedures and sign-in and visitor escort procedures.

2. Personnel security measures shall include authorization processes to assure appropriate, need-to-know access to information, background clearances appropriate to the level of access, adequate training and supervision of all personnel with access to consumer information, maintenance of records of access authorization, and formal discipline procedures including termination.

3. System Security shall ensure technical security services which guard data integrity, confidentiality and availability and which prevent unauthorized access to all data, including data that is transmitted over a communications network.

VIII. PROCEDURES

<u>WHO</u>	<u>DOES WHAT</u>
<p>WCHO Executive Director Washtenaw County Administrator Washtenaw County Community Support and Treatment Services Director</p>	<ol style="list-style-type: none"> 1. Appoint membership to Security Committee insuring representation from: <ul style="list-style-type: none"> Senior Management Information and Technology Services Professional Staff Office of Recipient Rights Risk Management Reimbursement Departments Records Management/Clerical Support Finance Departments 2. Appoint Committee Co-Chairs who shall serve as Security Officers for both entities. 3. Provide consultation to the Committee from Corporation Counsel, Human Resources, Provider Relations and Quality Improvement. The Committee is also given the authority to use specialized consultants from time to time to complete its work.

WHO

DOES WHAT

Security Committee

1. Establishes terms of membership
2. Meets regularly for routine business
3. Schedules additional meetings as needed to address specific concerns
4. Maintains minutes and other records of activities
5. Reports oversight activities and significant findings to the Executive Director of the WCHO and the Director of CSTS on a quarterly basis.
6. Conducts an annual risk assessment and risk analysis that includes:
 - a. Identification of assets
 - b. Assessment of potential risks, vulnerabilities and current controls, including threats to confidentiality, integrity and availability of information
 - c. Development of plans to address identified risks
 - d. Recommendations regarding expenditures to address identified needs, selecting cost effective control measures which balance the costs of proposed measures with the human and financial risks of potential loss and harmThe risk assessment shall be updated annually or whenever there is a significant change in circumstances.
7. Based upon the risk analysis and recommendations the committee:

Conducts an annual review of all related policies and procedures assure compliance with related laws, regulations, accreditation standards and professional ethics. This review will focus strictly on compliance with security of information and will not supplant other assigned responsibility for specific policies.
8. The committee will assure that policies and procedures address each of the following areas:
 - Privacy and confidentiality
 - Physical Safeguards/Physical Access Controls
 - Media controls
 - Workstation/Desktop Use
 - Technical Security Services
 - Training and monitoringThe committee will recommend changes or updates to policies and procedures to WCHO and CSTS management teams and other County Departments as indicated.
9. Provide coordination of compliance activities between WCHO and CSTS.
10. Provides oversight of education and training activities, coordinating information and efforts with Staff Development Committees and the County Professional Development Program. Training

shall include awareness training, periodic security reminders, user education, password management and reporting procedures.

11. Provides oversight of physical security measures and compliance, coordinating information and efforts with Safety Committees.
12. Reviews implementation plans for introduction of new data systems/elements with compliance implications
13. Reviews data related to any breaches of related policies and standards to determine appropriate systemic corrections and to assure that sanctions were applied appropriately