GHS/GCHC Computer Acceptable Use Agreement

Terms used throughout this document: CAUA - Computer Acceptable Use Agreement
GHS - Genesee Health System
GCHC - Genesee Community Health Center

A separate Computer Acceptable Use Agreement (CAUA) must be completed and signed for each provider entity (company) you work for, and you will be given a unique ID for each provider based on the job responsibilities specific to that provider. It is your responsibility to ensure you are signed on correctly at each location. In other words, while you are working for Provider A you must log in using the User ID assigned to you for provider A, not the User ID assigned for another provider.

WRITTEN AGREEMENT: I, (Staff Name) will

- use Electronic Health Record (EHR, e.g. CHIP or NextGen) or other GHS/GCHC computer systems on a need-to-know basis only
- retrieve or enter information about mutual clients as required for clinical care or business functions related to that clinical care only as it relates to my job duties and licensing
- take all reasonable precautions to protect the privacy of client information and will not leave display screens or printed materials containing client data where they could be viewed inappropriately
- change my password so it is known only to me and will keep it secure
- NOT disclose my password or allow another person to log in with my User ID and password
- NOT log on using someone else's User ID and password, I understand that doing so is fraud and not allowed in any circumstance

All users of GHS/GCHC computer systems are bound by this agreement.

Staff email Address		Phone Number	
Provider		Network Affiliations:	Mental Health
Programs		Primary Location	
Job Duties			
	Credentials after signature on billable documentation		
	Note: Please contact Genesee Health System (GHS) regarding any change in your licensure		

Note: It is the legal obligation of all CHIP users to protect access to medical records and protected health information by keeping your password secure.

Staff Type:

My signature below indicates that I have read and understood this document, including Attachments A (HIPAA) and B (HITECH), and I assure all credentials and supervision meet the requirements referenced in GHS Policy #02-000-99.

Staff Signature:		Date:

As Supervisor for this staff, my signature below indicates that I have read, understood and assure all credentials have been verified and meet the requirements referenced in GHS Policy #02-000-99.

Supervisor Name:		**Supervisor Credentials**:
Supervisor Signature:		Date:
Supervisor Email:		

Contracted Providers: HR contact send completed form to Provider Relations: **Fax #810-496-5770;** email **networkCAUA@genhs.org**

GHS/GCHC Direct Staff: Scan and email to "**CMHCAUA**"

GHS/GCHC Computer Acceptable Use Agreement for HR Designee

Attachment A: 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 system. 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.
You must have a separate ID for each provider, and it is your responsibility to ensure you are signed on correctly at each location. In other words, while you are working for Provider A you must log in using the User ID assigned to you for provider A, not the User ID assigned for another provider.
For more details see HIPAA Security Rule section # 164.312 (Technical Safeguards).

Attachment B: 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 now required to also comply. Business associates are required to report security breaches to covered entities consistent with the requirements, and are 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 breach 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 a 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 entity is investigating, mitigating and protecting against future breaches
5. A toll free telephone 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 unauthorized 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.