NorthStar System User Access Request

Type of Change	◯ New	◯ Change	◯ Inactivate	
Date of Request		Effective Date of Change		
User First & Last Name				
User Phone Number				
User Email Address				
User Title/Role				
Access Requested	☐ 837 Claim Files	☐ Manual Claim Entry	☐ Authorizations	☐ Clinical
MFA Device	◯ Agency Cell Phone	◯ Fob	◯ Personal Cell Phone	
Agency/Provider Name				
Site(s)				
Supervisor	Name			
	Phone		Email	

I agree to seek access only to client records, data, and information for which I have proper clearance and a need to know in order to perform the tasks assigned to me. Under no circumstances will I divulge the contents of any client's record or any other information of this organization to any person who does not have the proper clearance and a need to know.

As such, I realize that for security reasons all activity I perform in the Electronic Health Record systems of North Country Community Mental Health will be logged and auditable in the case of suspected violations of this agreement, HIPAA, or any other applicable laws.

The HIPAA Security Rule requires Covered Entities to implement "Unique User Identification" standard for electronic systems with Protected Health Information (PHI). Unique Use Identification is a unique name or number used to identify and track specific individuals using PHI systems, also referred to as "Login ID" or "User ID". This provides a means to verify the identity of the persons 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 is 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 user, and it is your responsibility to ensure you are signed on correctly at each location. For additional information, see the HIPAA Security Rule section 45CFR 164.312 (Technical Safeguards):

http://www.gpo.gov/fdsys/pkg/CFR-2010-title45-vol1/pdf/CFR-2010-title45-vol1-sec164-312.pdf

The HITECH Act imposes data breach* notification requirements for unauthorized uses and disclosures of "unsecured PHI" (Protected Health Information), (or 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 to up to $1.5 million.

The HITECH 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 and 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 the breach occurred. All required notifications must be made within ten (10) business days of the discovery of the breach to the Office of Recipient Rights at North Country Community Mental Health by calling 231-439-1268. The Business Associate will also comply with any formal requests from the covered entity regarding the breach, as well as fulfill any other obligations as stated in the HITECH Act.

*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.

By signing this agreement, you agree to abide by that which is stated above, and also agree to fulfil any obligations as set by the contract(s) between your employer and North Country Community Mental Health.

_____ _____

Signature of User Date

Management Staff:

As Manager of the above listed employee, my signature indicates that:

- I have read and understood this document and I assure that all stated requirements will be met
- I agree to inform North Country Community Mental Health immediately if the above listed employee no longer needs access rights to North Country Community Mental Health's system so that the appropriate security measures can be taken to discontinue access rights

_____ _____

Managing Staff Signature Date