North Carolina Department of Health and Human Services
Division of Medical Assistance

PROVIDER CONFIDENTIAL INFORMATION AND SECURITY AGREEMENT INSTRUCTIONS

Attention: Carolina ACCESS Primary Care Providers
Carolina ACCESS Enrollment, Referral, Emergency Room, and Utilization Reports

The Division of Medical Assistance's Managed Care Section is beginning the process of replacing paper copies of the Carolina ACCESS Enrollment, Referral, Emergency Room, and Quarterly Utilization reports with web-based versions of the reports. Each Carolina ACCESS Primary Care Provider (PCP) must complete the Provider Confidential Information and Security Agreement and return it to gain access to these web-based versions. Each approved user will receive log in information via email. This e-mail will include a link to the DMA Information and Report System http://reports.ncmedicaid.com where the user will have access to the following:

- Security Contact Administration
- On-line training
- Access to View Reports
- Technical Support
- Additional Information (related sites)

Instructions for Completing the Provider Confidential Information and Security Agreement

Only one Provider Confidential Information and Security Agreement shall be active for each enrolled Carolina ACCESS Primary Care Provider. If a practice is enrolled as a group, the practice must select one person as the Security Contact for the group. Likewise, if individual providers in a group practice have chosen to enroll with Carolina ACCESS individually, a Provider Confidential Information and Security Agreement must be completed for each individual provider enrolled. Providers MAY choose to select ONE Security Contact person for multiple practices or for more than one Carolina ACCESS provider number, but a form containing original signatures must be submitted for each active Carolina ACCESS provider number. The Security Contact person will be given the ability to add other users in the practice or network to the system so that they can access reports. The provider is responsible for the oversight of the Security Contact person's role.

1. **Carolina ACCESS Practice Provider's Enrollment Number:**
   The provider number on the Provider Confidential Information and Security Agreement must be the active Carolina ACCESS provider number because it drives the separation of the reports. Some of these reports include private health information (PHI) and are covered under the HIPPA Privacy Act for the patients listed on the reports. It is very important that a user is not granted access to a Provider Number he or she has not been approved access.

2. **Carolina ACCESS Practice Name:**
   Because the Carolina ACCESS practice name is used for verification when approving a user access to provider reports, it is important to list the practice name as it appears on the Carolina ACCESS application.

3. **Carolina ACCESS Practice Address:**
   The Carolina ACCESS practice address is also used for verification when approving a user access to Provider reports and must agree with the information provided on the Carolina ACCESS application.

4. **Provider's Security Contact Name (First, Middle, Last):**
   a) Security Contact Name must be printed clearly and listed exactly as it is listed on the Security Contact User's Social Security Card.
   b) The Social Security Administration is working to develop a (Pass/Fail) one-time verification whose sole purpose is to match a user with a Social Security Number. This verification will not be used in any other manner. Private information related to the Social Security Number will not be accessible or stored in any way. User's Social Security Numbers will not be posted anywhere for State or Provider Access. This process has been created to assure the validity of all users who will access PHI reports.
   c) Social Security Numbers will be linked to a user in a secure database on site. User names and Social Security Numbers will not be stored on any web site or shared servers. This process is being used to protect PHI system access as well as to protect the user.
   d) There is a possibility of approximately 3,000 to 5,000 users involved in the Carolina Access Web Portal release. The Carolina Access Project is the first of many projects providing this type of information concerning PHI across the State of North Carolina.
   e) This method of "identity management" (i.e., linking user name with SSN within a secure database) is extremely secure and reliable and is more assuredly in the best interest of both the State and the Provider.

5. **Security Contact Birth Date:**
   Birth Date is additional information requires for Provider Employee distinction.

6. **Provider's Security Contact Signature and Date:**
   The original signature of the designated Security Contact person and date are required to keep on file for Security and Federal audits.

7. **Provider Security Contact Person's Social Security Number:**
   Please see number (4) above. The User is protecting the practice by providing us with this information. With this information, we can assure that unauthorized access to the provider's reports and to patient PHI is eliminated. Accessing PHI via a Web Portal is a great step towards future Health Care if done so in a secure environment.

   Because sending passwords via e-mail is against HIPPA Security Rules, the Security Contact person will receive and e-mail containing the assigned user ID a message that the initial temporary password is the Security Contact person's social security number. At initial login, the user will be forced to change their password for additional security. DMA grants the Security Contact access to the appropriate provider reports and no one else sees the user's SSN.

8. **Provider Security Contact Person's e-mail:**
   We require an e-mail address so the Security Contact Person will be able to receive the log on information. If a Provider has internet access in the office, the user could set up an address to be used only for work-related purposes. In the future, the total DMA Information and Report System users could reach the tens of thousands and the State must make this process as electronic as possible. Once the user has been approved and access given, they will receive an email with information about the DMA Information and Report System and a link to this portal.

9. **Provider Witness of Security Contact Signature and Date:**
   The actual signature of the Carolina ACCESS Primary Care Provider and date signed is required to verify the provider has authorized this user to access the provider's reports. The signature must be that of an active Carolina ACCESS PCP listed on the Carolina ACCESS application for the corresponding practice and Carolina ACCESS provider number. This signature also authorizes the Security Contact person to set up or modify access of other users in the office. The appropriate signature is required for State and Federal Audits.

10. **DMA Sponsor and Date (DHHS OFFICE USE ONLY):**
    The DMA Sponsor who approves the Carolina ACCESS Contract or change in Provider Security Contact Person is required to sign and date on this line for State and Federal Audits.

North Carolina Department of Health and Human Services
Division of Medical Assistance

PROVIDER CONFIDENTIAL INFORMATION AND SECURITY AGREEMENT

The Provider understands that:

The identity of Medicaid applicants and recipients including, but not limited to, Medicaid identification numbers, names, and related medical health claim information is confidential protected health information and may only be disclosed in accordance with DHHS, state, and federal laws and regulations.

Each provider must delegate a staff member as the Security Contact Person who will be responsible for requesting user access to automated reports and resources. The Security Contact Person or Provider must also notify the Division of Medical Assistance (DMA) of any change in job duties, termination of employment, or leave of absence that would require immediate action for a user.

All passwords assigned to the provider and designated users for access to automated reports and resources are confidential. Logon identifiers and passwords uniquely identify the user. It is a violation of federal and state laws and regulations and the Department of Health and Human Services and DMA system security policy to divulge or share logon identifiers and passwords with another person.

To protect confidential data, the provider and designated users must safeguard and protect electronic data transactions that transmit protected health information about Medicaid applicants and recipients. The provider and designated users are responsible for ensuring that reasonable efforts must be made to protect the confidentiality of individually identifiable health information in all situations including e-mail, regular mail, fax, etc. All users with approved access to multiple Provider reports are responsible for accessing the data at the location specified by the approving provider.

DMA or its agents, will retain this original signed Agreement in the provider's file. Providers should copy and retain a copy of this agreement in their files.

The signature of the designated Provider Security Contact person and the Provider witness signifies that the Provider and the Security Contact person have read this Agreement and understand the obligations to protect confidential protected health information. The Provider further agrees that the rules and regulations pertaining to privacy and security mandated by the Health Insurance Portability and Accountability Act (HIPAA) of 1996 P.L. 104-91, as amended apply to the terms of this agreement and any agreements or practices executed by DMA or its agents to comply with HIPAA requirements.

□ Check if this is a change for your Designated Security Contact

*Carolina ACCESS Practice NPI Medicaid Provider Number

*Carolina ACCESS Practice Name *Phone Number (including area code)

*Street Address Line 1 (Site/Physical Address; not a P.O. Box)

Street Address Line 2

*City *State *Zip Code + Four (Last 4 digits required)

*Signature of Provider's Security Contact *Date

*Printed Name of Provider's Security Contact (Last, First, Middle) *Security Contact Date of Birth

*Security Contact E-mail Address *Security Contact Social Security Number

DMA Sponsor Date