



The Quality Times

PROMOTING QUALITY IMPROVEMENT THROUGH COMMUNICATION



Who, What, Where, & Sometimes Why

November/December 2009

Critical Access Behavioral Healthcare Agency: What is it?

As a result of budget reductions, the Division of Mental Health, Developmental Disabilities and Substance Abuse Services has looked for methods to improve service delivery within the environment of more limited public funding for services. The most current initiative is the proposal of a new comprehensive service delivery entity known as a Critical Access Behavioral Healthcare Agency (CABHA). The CABHA has been proposed to create more cohesive service arrays within provider networks across the state. CABHA organizations will be permitted to provide case management services to recipients of MH/DD/SA services. All agencies who want to provide enhanced services that have a case management component bundled will need to meet these requirements (this does not include DD Targeted Case Management).

There are several requirements that make an agency eligible to be designated a CABHA. Generally, there are staffing/administrative requirements, and standards for the continuum of services that are being provided by that agency. CABHA organizations must have met a minimum 3 year accreditation from a state approved accrediting body.

Staffing Requirements—At the minimum, each agency will need to have a:

Medical Director: Whether or not this is a full or part time position will be dictated on how many consumers are served by the agency. This position must be occupied by a licensed physician or psychiatrist.

Clinical Director: This is a full time position that must be occupied by a fully licensed clinician. A provisionally licensed individual would not be eligible to serve as an agency's clinical director.

Quality Improvement/Training Director: This full time position will be responsible for ensuring organizational compliance regarding staff credentials, documentation, etc. Additionally, this director will be responsible for collecting and maintaining data to track treatment outcomes that may be compared to other similar providers.

Service Array:

In order to be eligible to be certified as a CABHA, an organization must be able to offer a continuum of services ranging from basic benefits to enhanced services. Clinicians must offer comprehensive assessments, outpatient therapy and medication management. A CABHA must also be endorsed to provide 2 enhanced services (such as Intensive In-Home and MST). These services must form a logical continuum and be based on sound clinical practice. CABHA must be willing to accept both Medicaid and IPRS funded consumers to their practice.

Inevitably, there will be more information regarding these organizations in the near future and we will attempt to keep our provider network informed as new information is released. Continue to check DMA and DMH for the most current information.

DMA “Top Ten” reasons for Delayed Processing of an Enrollment Application

In the December 2009 Medicaid Bulletin, DMA has compiled a list of common errors which are preventing a DMA enrollment application from being processed without delay. Please note these common errors and try to avoid them. In doing so, there is a greater chance that your agency could be assigned a DMA enrollment number sooner, rather than later.

TOP 10

The issues reported were as follows:

1. The W-9 form is not filled out correctly.
2. Section 18 A and B of the ownership and managing em-

- ployees form are not provided.
3. The indicator boxes are not marked.
4. Titles are not provided.
5. Required documents are not provided.
6. Documents that have been returned are incorrect.
7. A DMA Provider Services Business Rule requirement is not met.
8. An administrative review is needed.
9. The provider has not responded to e-mails and return letters.
10. The signer is not an authorized agent for the provider.

In other instances, a provider's application may be completely rejected—causing an entirely new application to be submit-

ted. The following are the top 3 most common reasons for this circumstance:

1. The wrong type of application is submitted.
2. The wrong version of an application is used.
3. An enrolled provider has submitted a new application instead of a change form.

Thank you for your attention to these matters. By proactively avoiding these common mistakes, it may be possible to receive your enrollment confirmation sooner than if there is a small issue holding up the process.

Community Support Case Management to continue into 2010

Due to delays in the development of a case management service definition, the Centers for Medicare and Medicaid Services has approved a request to continue the case management component of community support services for the foreseeable future. This component of Community Support may only be provided by a Licensed Professional or a Qualified professional.

After January 1, 2010, any new requests for Community Support will only be permissible under the case management component of the service. Consumers who are receiving

Community support will be able to receive all aspects of the service until the end of their authorization period, at which point a reauthorization would be for case management services only.

The maximum authorization for Community Support case management will be four hours per month. PCPs submitted to Value Options must document medical necessity for case management and the plan must include case management specific goals that will be addressed. Any therapeutic, psycho-educational or skill based goals must be removed

from the PCP before submission.

Please review Implementation Update #65 for a complete list of functions which may be provided under the case management component of CSS.

If additional time is required for children, the EPSDT process is an option that could be used. Please see the guidelines at:

<http://www.dhhs.state.nc.us/dma/epsdt>



Red Flag and Address Discrepancy Rule

OPC recently forwarded information to providers related to the “Red Flag and Address Discrepancy Rule”. Below is an article published by the Federal Trade Commission with more information specific to health care providers. You can also find this article at: <http://www.ftc.gov/bcp/edu/pubs/articles/art11.shtm>

The “Red Flags” Rule: What Health Care Providers Need to Know About Complying with New Requirements for Fighting Identity Theft

by Steven Toporoff - attorney with the FTC's Division of Privacy & Identity Protection

As many as nine million Americans have their identities stolen each year. The crime takes many forms. But when identity theft involves health care, the consequences can be particularly severe.

Medical identity theft happens when a person seeks health care using someone else's name or insurance information. A survey conducted by the Federal Trade Commission (FTC) found that close to 5% of identity theft victims have experienced some form of medical identity theft. Victims may find their benefits exhausted or face potentially life-threatening consequences due to inaccuracies in their medical records. The cost to health care providers — left with unpaid bills racked up by scam artists — can be staggering, too.

The Red Flags Rule, a law the FTC will begin to enforce on November 1, 2009, requires certain businesses and organizations — including many doctors' offices, hospitals, and other health care providers — to develop a written program to spot the warning signs — or “red flags” — of identity theft. Is your practice covered by the Red Flags Rule? If so, have you developed your Identity Theft Prevention Program to detect, prevent, and minimize the damage that could result from identity theft?

WHO MUST COMPLY?

Every health care organization and practice must review its billing and payment procedures to determine if it's covered by the Red Flags Rule. Whether the law applies to you isn't based on your status as a health care provider, but rather on whether your activities fall within the law's definition of two key terms: “creditor” and “covered account.”

Health care providers may be subject to the Rule if they are “creditors.” Although you may not think of your practice as a “creditor” in the traditional sense of a bank or mortgage company, the law defines “creditor” to include any entity that regularly defers payments for goods or services or arranges for the extension of credit. For example, you are a creditor if you regularly bill patients after the completion of services, including for the remainder of medical fees not reimbursed by insurance. Similarly, health care providers who regularly allow patients to set up payment plans after services have been rendered are creditors under the Rule. Health care providers are also considered creditors if they help patients get credit from other sources — for example, if they distribute and process applications for credit accounts tailored to the health care industry.

On the other hand, health care providers who require payment before or at the time of service are not creditors under the Red Flags Rule. In addition, if you accept only direct payment from Medicaid or similar programs where the patient has no responsibility for the fees, you are not a creditor. Simply accepting credit cards as a form of payment at the time of service does not make you a creditor under the Rule.

The second key term — “covered account” — is defined as a consumer account that allows multiple payments or transactions or any other account with a reasonably foreseeable risk of identity theft. The accounts you open and maintain for your patients are generally “covered accounts” under the law. If your organization or practice is a “creditor” with “covered accounts,” you must develop a written Identity Theft Prevention Program to identify and address the red flags that could indicate identity theft in those accounts.

SPOTTING RED FLAGS

The Red Flags Rule gives health care providers flexibility to implement a program that best suits the operation of their organization or practice, as long as it conforms to the Rule's requirements. Your office may already have a fraud prevention or security program in place that you can use as a starting point.

If you're covered by the Rule, your program must:

Identify the kinds of red flags that are relevant to your practice;

Explain your process for detecting them;

Continued from page 3

Describe how you'll respond to red flags to prevent and mitigate identity theft; and

Spell out how you'll keep your program current.

What red flags signal identity theft? There's no standard checklist. Supplement A to the Red Flags Rule — available at [ftc.gov/redflagsrule](https://www.ftc.gov/redflagsrule) — sets out some examples, but here are a few warning signs that may be relevant to health care providers:

Suspicious documents. Has a new patient given you identification documents that look altered or forged? Is the photograph or physical description on the ID inconsistent with what the patient looks like? Did the patient give you other documentation inconsistent with what he or she has told you — for example, an inconsistent date of birth or a chronic medical condition not mentioned elsewhere? Under the Red Flags Rule, you may need to ask for additional information from that patient.

Suspicious personally identifying information. If a patient gives you information that doesn't match what you've learned from other sources, it may be a red flag of identity theft. For example, if the patient gives you a home address, birth date, or Social Security number that doesn't match information on file or from the insurer, fraud could be afoot.

Suspicious activities. Is mail returned repeatedly as undeliverable, even though the patient still shows up for appointments? Does a patient complain about receiving a bill for a service that he or she didn't get? Is there an inconsistency between a physical examination or medical history reported by the patient and the treatment records? These questionable activities may be red flags of identity theft.

Notices from victims of identity theft, law enforcement authorities, insurers, or others suggesting possible identity theft. Have you received word about identity theft from another source? Cooperation is key. Heed warnings from others that identity theft may be ongoing.

SETTING UP YOUR IDENTITY THEFT PREVENTION PROGRAM

Once you've identified the red flags that are relevant to your practice, your program should include the procedures you've put in place to detect them in your day-to-day operations. Your program also should describe how you plan to prevent and mitigate identity theft. How will you respond when you spot the red flags of identity theft? For example, if the patient provides a photo ID that appears forged or altered, will you request additional documentation? If you're notified that an identity thief has run up medical bills using

another person's information, how will you ensure that the medical records are not commingled and that the debt is not charged to the victim? Of course, your response will vary depending on the circumstances and the need to accommodate other legal and ethical obligations — for example, laws and professional responsibilities regarding the provision of routine medical and emergency care services. Finally, your program must consider how you'll keep it current to address new risks and trends.

No matter how good your program looks on paper, the true test is how it works. According to the Red Flags Rule, your program must be approved by your Board of Directors, or if your organization or practice doesn't have a Board, by a senior employee. The Board or senior employee may oversee the administration of the program, including approving any important changes, or designate a senior employee to take on these duties. Your program should include information about training your staff and provide a way for you to monitor the work of your service providers — for example, those who manage your patient billing or debt collection operations. The key is to make sure that all members of your staff are familiar with the Rule and your new compliance procedures.

WHAT'S AT STAKE ?

Although there are no criminal penalties for failing to comply with the Rule, violators may be subject to financial penalties. But even more important, compliance with the Red Flags Rule assures your patients that you're doing your part to fight identity theft.

Looking for more information about the Red Flags Rule? The FTC has published [Fighting Fraud with the Red Flags Rule: A How-To Guide for Business](https://www.ftc.gov/redflagsrule), a plain-language handbook on developing an Identity Theft Prevention Program. For a free copy of the Guide and for more information about compliance, visit [ftc.gov/redflagsrule](https://www.ftc.gov/redflagsrule).

In addition, the FTC has released a fill-in-the-blank form for businesses and organizations at low risk for identity theft. The online form offers step-by-step instructions for creating your own written Identity Theft Prevention Program. You can fill it out online and print it. The do-it-yourself form is available at [ftc.gov/redflagsrule](https://www.ftc.gov/redflagsrule).

Questions about the Rule? Email RedFlags@ftc.gov.

PCP DEVELOPMENT

Due to the reduction and eventual elimination of community support, a greater variety of providers may now be responsible for developing Person Centered Plans (PCP) for the consumers they would like to serve. Services such as Level 2 Therapeutic foster care, Day Treatment and Psychosocial Rehabilitation will no longer be required to have a community support worker to develop and monitor the PCP.

Only a qualified professional delivering the service may develop the PCP. The QP who has developed the PCP must receive the state mandated trainings—Person Centered Thinking (6 hours) and PCP Instructional Elements (3 hours). If the agency developing the PCP is not designated as a “first responder”, the QP must collaborate with the area LME to identify community based resources to be accessed in the event of a crisis.

Q-Tips

- *Check the DMH and DMA websites regularly for updates.*
- *Please remember that you must begin providing enhanced services to consumers within 60 days of enrollment with DMA. LMEs have been instructed to involuntarily withdraw endorsement if service provision has not begun within this timeframe.*
- *The Division of MH/DD/SAS has added a “Records Management” page to it’s website. Please visit this page at:*

<http://www.ncdhhs.gov/mhddsas/recordsmgmt/index.htm>

Be on the look out...

As stated in IU #63, the process to re-verify information and credentials of enrolled Medicaid Community Intervention Services providers is scheduled to begin immediately. Computer Sciences Corporation (CSC) will be notifying providers by mail and sending the notification packet to the provider's billing/accounting address. This will include a pre-printed report of information currently on file with N.C. Medicaid plus a checklist of credentialing-related documents that must be returned to CSC.

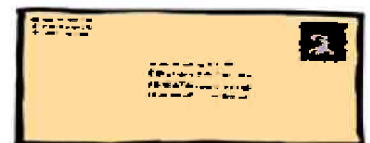
The pre-printed form which all enrolled providers will be receiving will include the demographic information that DMA currently has on file. Please review and change any information which needs to be updated. A response is required within 30 days of receiving the form.

According to CSC, The verification process will take up to three weeks from the time CSC receives the correct and complete verification packet from the provider; the

return of incomplete or incorrect information may lead to an interruption in enrollment. Lack of compliance in these procedures could result in suspension of enrollment and eventual termination.

CIS providers who are enrolled for Community Support Team should take special note for these processes. In order to continue enrollment, current NEA letters must be submitted along with the required staff credentials and licensure information.

If you do not receive the notice in the mail you may verify your billing/accounting address via the DMA Provider Services NPI and Address Database at <http://www.ncdhhs.gov/dma/WebNPI/default.htm> or by calling the EVC Call Center at 1-866-844-1113



WELCOME

OPC Area Program has a new Guardianship Coordinator! Laura McKay has joined the QI-PR department from her former role in Care Coordination to accept the challenge of managing and coordinating care for wards who OPC has been named guardian. If you provide care for an individual who OPC serves as guardian, please feel free to contact Laura with any questions you may have regarding their care. She can be reached at 919-913-4036 or via email at lmckay@opc-mhc.org. We are lucky to have her join us.

The QI-PR department is happy to welcome a new administrative assistant to our team. Naomi Avissar has joined us and will be responsible for medical records storage, gun permits and training registration at the current time. Please feel free to contact her for the above mentioned issues at (919) 913-4053. She can be reached via email at navissar@opc-mhc.org.

Upcoming OPC Trainings and Events

January 1st, 2010
 OPC Area Program Administrative Offices Closed
 Celebrating 2010

February 10, 2010
 Client Rights and Confidentiality
 Europa Center, 1pm-4pm

January 11, 2010
 OPC Board Meeting
 Europa Center, 7pm

March 12th, 2010
 Incident Reporting
 Europa Center, 1pm-4pm

January 27th, 2010
 Documentation Training
 Europa Center, 1pm-4pm



March 17th, 2010
 Understanding the DSM-IV-TR
 Europa Center, 1pm-4pm, \$25 (CEUs Offered)

Please visit our online event calendar for more information on upcoming events at: <http://www.opcareaprogram.com/calendar/january2010.html>

If you would like information added onto our event calendar, please notify your provider representative.
 For questions, please contact Naomi Avissar at (919) 913-4053