MITS is LIVE!

The Ohio Medicaid Information Technology Information System (MITS) went live on August 2, 2011. MITS will process claims more quickly and accurately than ever before. It will allow Ohio to better manage Ohio Medicaid's business processes and meet upcoming federal guidelines for state Medicaid programs. Provider Information Releases, Supplemental Releases and Reminder Releases have informed Ohio's Medicaid providers of changes that would be coming with MITS. In addition, more than 200 training sessions have been offered around the state to help providers prepare for the new system. The MITS website continues to be updated frequently with provider information and training resources, as well as system updates.

Although MITS will improve Ohio's Medicaid program, providers may notice some changes that may cause interruptions in day-to-day operations. Many information releases and training resources have been and will continue to be available on the MITS website to help providers through the transition. Now that the new system is in full production, it will be updated periodically for improved functionality. It is important that providers stay informed about all MITS updates, issues and changes by going to http://jfs.ohio.gov/mits/index.stm.

We encourage providers to use the tools that are available to them online prior to calling the Provider Call Center. This will enable the Call Center to better assist providers with questions that are not addressed on the website.

Throughout this information release you will find new information to help clarify some of the known issues and resolutions, and additional information that has been requested by the provider community.

Additional Provider Training

If you or your organization has new employees who were not able to attend any of the pre-implementation provider trainings held in the fall of 2010 or the summer of 2011, additional trainings are available. Please go to http://jfs.ohio.gov/mits/MITS_Provider_Training_Fall_2011.pdf for registration information.

MITS Web Portal

One of the greatest enhancements for providers is the MITS Web Portal. The new portal provides online submission and management for dental, professional and institutional claims. Below are several tips to remember when setting up your new MITS Web Portal account.

Creating a New MITS Account

When creating a User ID for your organization's MITS provider administrator account, keep in mind that the account is owned by the provider and not the person who is setting up the administrator account. Whatever User ID is created will remain the same for the provider number, which is also the Medicaid billing number. It is recommended that the provider User ID be recognizable to the account administrator and not to other agents. For example, for an organization called Okay Home Health, it would make more sense to make the User Name OKHHeal1 than JaneDoe1. This will also help employees remember which User ID is for the portal account administrator and which is for the agent.

Creating Agent User IDs

Agents should create their own User IDs and passwords. This will allow them to remember the User IDs and passwords more easily, which will reduce the number of lockouts that occur as a result of repeatedly entering incorrect information.

The MITS Web Portal was created to be role-based at the agent level. Agents can access provider information only after the account administrators assign them specific roles.

Issue: Unable to locate agent User ID when trying to assign roles through the Account Maintenance function

If the administrator is assigning agents to roles but is unable to locate an agent within the Account Maintenance panels, this could be because the agent has not clicked on the "Secure Portal" link, or the agent may have used a different User ID or created the account using a different name. If either of those situations occurred, please take the following steps:

- If the agent has not logged in to his or her Agent ID and clicked on the "Secure Portal" link, *ask him or her to do so. Then conduct a new search to locate the agent.*
- If the agent has a different User ID or created the account using a different name, *double-check both the User ID and the spelling of the agent name and try again.*

Issue: Agent unable to see roles that were assigned for a provider

If an agent does not see the assigned roles for a provider (for example, eligibility, claims, prior authorization or 1099 roles), this is because the agent has not selected a default provider within the "Switch Provider" feature through the agent account. In the Switch Provider panel, the agent should click on one of the provider numbers that appear on the panel and, when the provider information is populated below the line chosen, click on the "Default" check box.

Deleting Agents

If a User ID is no longer needed, then it is necessary to determine the type of User ID that it is to discuss the removal of User IDs. User IDs will be disabled after 90 days of inactivity. Below describes the two different types:

Administrator/Provider

The Administrator/Provider User ID has a one-on-one relationship with the Medicaid provider number it was created under. This means one User ID to one Medicaid provider number. Due to this direct association the action of deleting a User ID is not available for the Administrator/Provider User IDs.

Agent

The MITS Secure Portal was created to be role based at the agent level. An agent User ID does not have any access to provider information until an administrator of a provider assigns specific User IDs roles. If an agent is no longer associated with a provider (no longer with the organization or no longer in a role that requires access), then the account administrator needs to follow the steps below to remove all access from the agent for that provider account:

1) Go into the Agent Maintenance panel;
2) Find the agent who no longer needs access;
3) Select the "Remove Agent" button.

If the need is to delete an agent User ID as it is no longer necessary or someone had multiple agent accounts, removing all roles specific to the one User ID deletes the access. An agent User ID cannot be deleted from the system as it has an historical value within the MITS.

Security Questions

It is highly recommended that all agents and account administrators complete the security questions when setting up User IDs. Each type of account gets only three attempts to log in before the account is suspended, to safeguard its security. If you have completed the security questions, then after two failed log-in attempts you can click on the "Forgotten Password" option from the Sign In page. This will save your organization time by not having to wait for a password reset.

Issue: The User ID you have chosen has already been selected; please select a new User ID. (Formerly: User ID Already in Use)

When setting up either a provider administrator or an agent account, if you receive the message "User ID Already in Use" or "the User ID you have chosen has already been selected; please select a new User ID," this means that another person has already chosen and activated that User ID. You must choose another User ID. If this happens, do not call and ask for a password to be reset. Doing so will lock out the true owner of the account.

Issue: This Account has already been set up

When setting up a provider administrator account, if you receive the message "This account has already been set up," this means that another person has already set up the administrator account tied to that Medicaid ID. There can be only ONE administrative account per billing NPI. If you get this message, do not call and ask for a password to be reset. It will lock out the true owner (administrator) of the account.

If you believe you should be the administrator on the account, contact the help desk for assistance. If you are not the administrator on the account, then please exit the provider set-up page and proceed to the agent set-up page.

Number of User IDs Agents Can Have

Although there is nothing to prevent a user from creating multiple User IDs, technically agents need only one agent User ID. Even if agents work for two different providers, they still need only one agent User ID. (They will use the "Switch Provider" feature to move from one provider's account to another; the providers will be able to view their accounts only.) Having only one User ID also makes it easier for agents to remember their passwords. Agents with more than one User ID are advised to use only one User ID at a time, so as not to confuse which roles they have been assigned by each provider.

Account administrators may choose to set themselves up as agents, too, if their work requires them to do more than manage the agent roles for multiple provider numbers – for example, if they also do claims research, eligibility verification or prior authorization. That way, they can use the "Switch Provider" feature to move between accounts.

Issue: Invalid Credentials

If a user receives the error message "Invalid Credentials," this means that the account has been locked and a password reset is necessary. To request a password reset, call 1-800-686-1516 or email MITS_Access_Support@jfs.ohio.gov.

Issue: PIN has expired

If while attempting to set up an administrator account you receive the message "PIN has expired. Please reset PIN," email MITS_Access_Support@jfs.gov. The PIN itself is not needed in the email, but please include the provider number associated with the PIN. The new PIN will continue to be either the last four digits of the Employer Identification Number or Social Security Number.

Issue: Account administrator will be leaving or has left the organization or position

There are two ways to change ownership of the administrator account:

Planned Exit

While the former owner is still present, ask that person to log on to the administrator account and change the email and contact information to the new owner. The former owner should also change both the password and security answers to something general and share them with the new owner. The new owner should then log on with the new password. Once in the system, the new owner should change the password and security questions once again, to something that he or she will easily remember. *The above steps should never be taken for agent accounts.*

Unplanned Exit

If the former owner is no longer present, and the account information is unknown, please send an email to MITS_Access_Support@jfs.ohio.gov.

Claim Attachments for Electronic Claims

The new Internal Control Numbers (ICNs) can tell a lot about the way a claim was submitted. The first two numbers, called the Region Code, tell if the claim was received through an EDI 837 transaction, through the MITS Web Portal or on paper. In addition, the region code also indicates whether the claim had an attachment indicator completed or an attachment uploaded with a claim.

If an EDI claim begins with a 20, this indicates that the claim was submitted via an 837 transaction without the PWK segment (attachment indicator) populated within the 837 transaction. The 20 region code signifies an EDI claim without attachment. Using the PWK segment (attachment indicator) on an EDI claim will allow the claim to receive an ICN that begins with a 21 region code. The 21 region code indicates an 837 claim with attachments. An electronic claim must have the indicator completed if an attachment is to be associated with a claim. The 21 region code will trigger the claim to suspend until the document can be uploaded through the MITS Web Portal or until the claim can be matched to mailed documents with a completed EDMS cover sheet.

There is no way to match an attachment to a claim that begins with the region code 20 or 22 (portal claim, no attachment). Claims with attachments submitted through the MITS Web Portal will begin with region code 23. A list of all the major region codes is available to all providers at http://jfs.ohio.gov/mits/MITS_Internal_Control_Number.pdf.

Third-Party Liability, Coordination of Benefits and Crossover Claims

In order to understand how MITS processes other payer information, it is important to understand the two ways claims can be processed for payment by government or private carriers. When a claim is paid at the header level, this means that all the details on the claim are processed in a lump sum payment. Examples are claims processed by Diagnosis Related Group (DRG) or Ambulatory Surgery Center (ASC). However, if claims are paid at the detail level, then each line item on the claim is individually examined and decided whether to be paid, partially paid or denied.

Prior to submitting claims that have other payer information associated with them, it is important to look on the Explanation of Benefits or Explanation of Medicare Benefits to determine how the claim was processed.

For the most up-to-date information about MITS, provider training resources and notices pertaining to the new system please go to http://jfs.ohio.gov/mits/index.stm.

For more information for Medicaid providers and trading partners, please go to http://jfs.ohio.gov/OHP/index.stm.