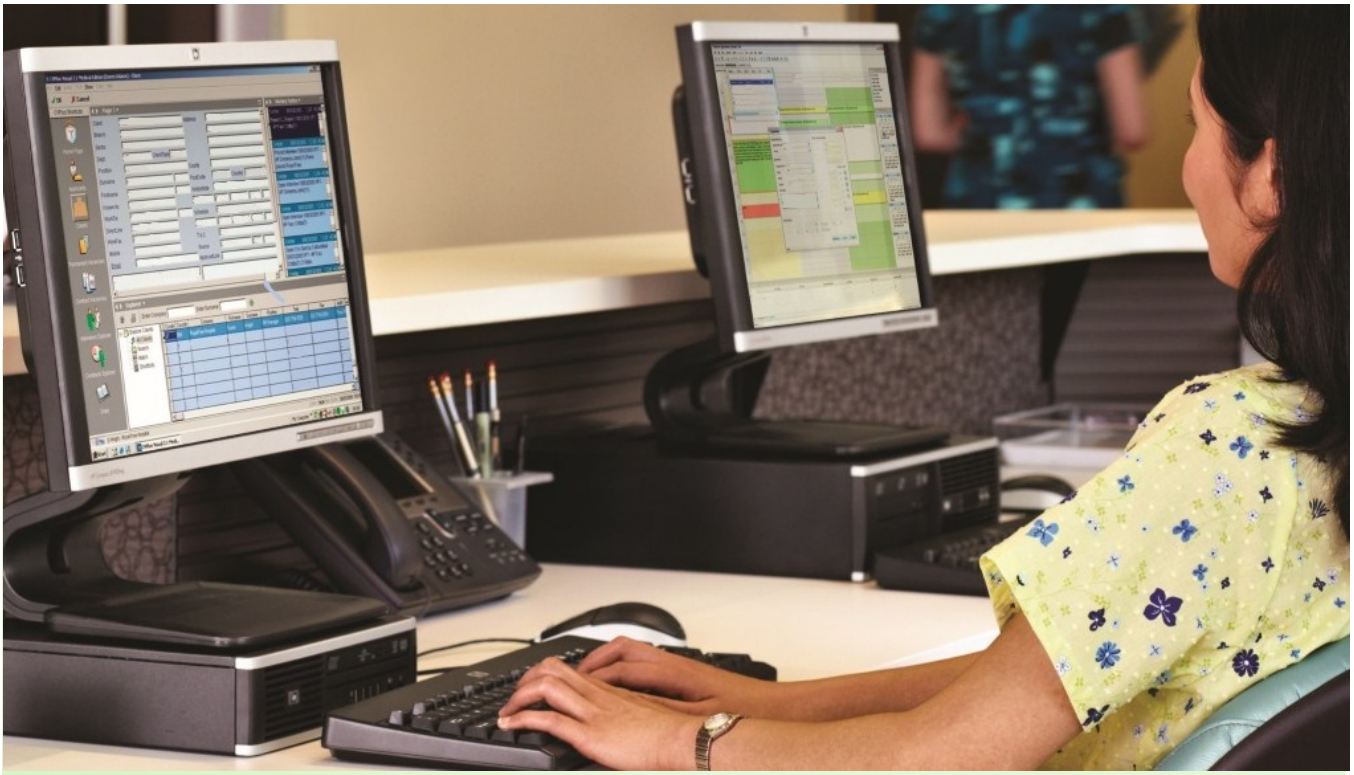
IHCP *bulletin*

INDIANA HEALTH COVERAGE PROGRAMS BT201242 OCTOBER 30, 2012



The IHCP updates Web interChange security policies and clarifies responsibilities

To ensure compliance with the *Health Insurance Portability and Accountability Act* (HIPAA) and better protect Indiana Medicaid data, the Indiana Health Coverage Programs (IHCP) continues to update its security policies. Compliance with security provisions requires providers be aware of HIPAA rules, IHCP policies, and the roles and responsibilities of Web interChange users, administrators, and provider owners.

New Web interChange password reset policy is effective December 1, 2012

The IHCP allows Web interChange users to reset their own passwords. The help window on Web interChange includes an Automated Password Reset document with detailed instructions on the process. If attempts to reset passwords are unsuccessful, users must contact their organization's Web interChange administrator for help. If users are not sure who their organization's administrator is, they can use the Administrator Listing link on the Web interChange log-on screen to obtain that information. If a user bypasses his or her organization's administrator and contacts the HP EDI Solutions help desk directly, the user is referred to his or her Web interChange administrator.

Under current practice, if an administrator is unable to help a user with a password reset, the EDI Solutions help desk

Continue

resets passwords for users over the telephone. **Effective December 1, 2012, passwords will no longer be reset over the telephone by the EDI Solutions help desk.** Under the new policy, after the user correctly answers his or her security questions, the EDI Solutions help desk will email a new temporary password to the user's email address on file. The user will be prompted to change the temporary password the first time he or she logs on.

Clarification of Web interChange roles and responsibilities

When a provider organization is given access to Web interChange, the organization's owner is required to approve the person selected as the Web interChange administrator. No user is given administrative access without authorization from the provider's owner. The term "owner" refers to the highest authority within an organization. In larger organizations, the "owner" could be the chief executive officer or someone of similar rank. In smaller organizations, the "owner" could be the organization's actual owner.

The Web interChange administrator is the first point of contact for users within an organization for issues regarding Web interChange access. It is highly recommended that each organization designate a backup administrator in case the primary administrator cannot be contacted.

There may be a number of Web interChange users within an organization. Users should be authorized to access data at the minimum level necessary to perform their job functions. Each user has a User Profile within Web interChange that includes user information specific to that individual.

Owner responsibilities – While the organization's owner does not have to be a Web interChange user, he or she should be familiar with Web interChange and how it is used within his or her practice. The owner must also understand the responsibility he or she assumes when designating a Web interChange administrator for his or her organization. Owner responsibilities include:

- Designating the Web interChange administrators for the organization

Continue

It is a HIPAA violation to share Web interChange IDs and passwords!

All users must safeguard their Web interChange user IDs and passwords. Each Web interChange user must have his or her unique user ID and password. Users are not allowed to share IDs, passwords, or security challenge questions with individuals inside or outside their organizations.

Sharing user IDs and passwords violates HIPAA security regulations and your Web interChange user agreement. The personal information associated with a user ID must belong only to that specific user. The user ID, password, security questions and answers, email address, and other contact information must pertain only to the individual user.

If the EDI Solutions help desk is notified that an administrator has left an organization and a letter has not been received from the owner requesting that the administrator be terminated, the EDI Solutions help desk will de-activate the administrator's user ID and contact the organization's owner to verify the administrator's status within the organization.

- Being responsible for all actions performed by the authorized administrators within the organization, and consequently, taking responsibility for the actions of all users under the administrators' authority
- Notifying the HP EDI Solutions help desk at (317) 488-5160 in the Indianapolis area or 1-877-877-5182 (toll free), or via email at INXIXElectronicSolution@hp.com, when administrative access needs to be removed or changed – The owner must submit a letter on company letterhead requesting removal or assignment of an administrator. The letter must be signed by the owner and mailed to 950 North Meridian Street, Suite 1150, Indianapolis, IN 46204 or faxed to (317) 488-5185. When an administrator leaves the organization, his or her access cannot be left open and cannot be transferred to a new administrator. The owner must designate a new administrator and establish new administrative access.
- Responding to the quarterly owner email – Using the owner's email address on file, a quarterly report is emailed to every provider owner, listing their organization's Web interChange administrators. The owner must verify that the list of administrators is correct. This will ensure appropriate access to the organization's data on the website. If the administrators listed in the email are incorrect, the owner must immediately contact the HP EDI Solutions help desk at (317) 488-5160 in the Indianapolis area or 1-877-877-5182 (toll free), or via email at INXIXElectronicSolution@hp.com to make corrections.
- Notifying the HP EDI Solutions help desk at (317) 488-5160 (local) or 1-877-877-5182 (toll free), or via email at INXIXElectronicSolution@hp.com of any changes to the owner email address on file.

Continue

Administrators must view their Group Reports to ensure the list of users is accurate and that users have correct permissions for their job functions.

To view the organization's group report, the administrator must:

1. Log on to Web interChange.
2. Click **Administration Menu**.
3. Click **Administer Groups**.
4. In the Top Level Group Information section, click **View Group Report**. The screen lists all users within the organization. The administrator must review the list and determine whether any action needs to be taken for the users listed.
5. After the administrator has reviewed the list of users, their status, and their permissions, the administrator must click the **Group Report(s) Reviewed** button at the bottom of the page. The system logs the date and time that the administrator viewed the group report.

Note: If it becomes evident that Web interChange administrators are not viewing their group reports at least every 90 days, additional security measures will be enforced.

Administrator responsibilities – Web interChange administrators are designated by the organization's owner. The administrator has a number of responsibilities that are necessary to ensure HIPAA compliance and data security. Administrator responsibilities include:

- Creating user access for your organization, including a unique user ID and temporary password
- Monitoring user activity to ensure that users in the organization are not sharing user IDs, passwords, or security questions and answers
- Taking responsibility for the actions of authorized users, as well as their own
- Assigning users to specific Web interChange levels of access (known as child-level groups)
- Ensuring that users are placed in appropriate groups and are granted access only to the minimal data necessary to perform their job functions
- Removing users from groups when they leave the organization or no longer need access
- Educating users about how to reset their passwords and helping users reset passwords
- Re-activating users who have been suspended due to lack of use
- Reviewing the access of all users on the group report every 90 days at a minimum – From the Group Report Administration page, the administrator can get a snapshot of all levels of access for users within his or her organization. See the callout box on page 3 for instructions.

User responsibilities – Users must be conscientious about safeguarding the security of their Web interChange access. User responsibilities include:

- Completing a Web interChange Access Request Form to establish a User Profile, including the user ID, telephone number, email address, name, and two security reset questions and answers specific to that individual. This request form is submitted to the user's Web interChange administrator.
- Updating the User Profile, as needed
- Resetting passwords, as appropriate
- Keeping passwords and security questions and answers secure

Continue

The IHCP encourages providers to take the following actions:

- **Owners** – Notify the HP EDI Solutions help desk of any changes to the owner email address on file; designate a backup administrator in case the primary administrator cannot be contacted.
- **Administrators** – View your Group Report to ensure that the list of current users is accurate and that users have correct permissions for their job functions.
- **Web interChange users** – Update your User Profile and make sure the email address listed there is correct.

For additional information on security policies, please visit Web interChange via indianamedicaid.com. This site includes online guidance, frequently asked questions, and other information to help users. If you need additional help or training, contact your HP field consultants. To find the field consultant for your area, visit the Provider Relations Field Consultants page on indianamedicaid.com.

To ensure HIPAA compliance and the security of Indiana Medicaid data, the IHCP continues to review its user ID and password policies. If the IHCP further modifies its security policies, Web interChange users will be notified via bulletin.

QUESTIONS?

If you have questions about this publication, please contact Customer Assistance at (317) 655-3240 in the Indianapolis local area or toll-free at 1-800-577-1278.

COPIES OF THIS PUBLICATION

If you need additional copies of this publication, please download them from indianamedicaid.com. To receive email notices of future IHCP publications, subscribe to IHCP Email Notifications.