National Practitioner Data Bank
Healthcare Integrity and Protection Data Bank

U.S. Department of Health and Human Services
HRSA Health Resources and Services Administration

FACT SHEET ON USER IDs AND PASSWORDS

Internet Querying and Reporting

Registered entities with active querying and reporting privileges and authorized agents on behalf of registered entities use the Data Banks and the internet based Integrated Querying and Reporting Service (IQRS) to query and/or report to the National Practitioner Data Bank (NPDB) and the Healthcare Integrity and Protection Data Bank (HIPDB).

The Data Banks are a national flagging system that help protect the public by disclosing adverse actions, taken against health care practitioners, providers, and suppliers, to authorized health care entities. The Data Banks also help safeguard against practitioners moving from State-to-State or job-to-job without disclosing their past history.

For information about IQRS security features, system requirements, and instructions for use, see the *Fact Sheet on the Integrated Querying and Reporting Service (IQRS).*

Logging in to the IQRS

The IQRS *Login* screen (Figure 1) has three fields that must be completed to access the IQRS. Enter your Data Bank Identification Number (DBID), User ID, and User Password into the corresponding fields and click **Login**. The User Password and User ID fields are case sensitive.
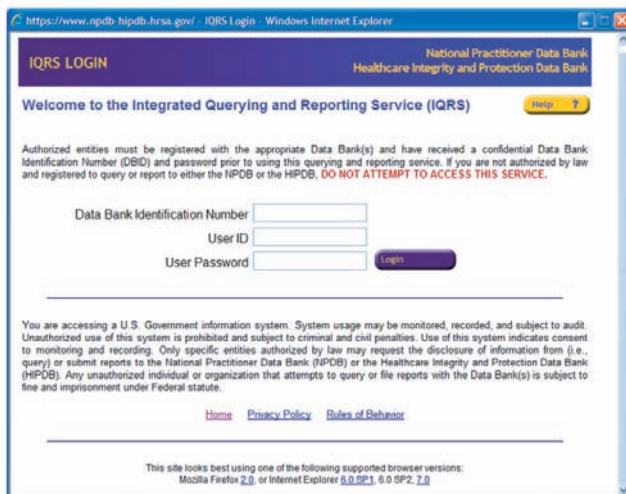

Figure 1. Login Screen

Creating and Maintaining User Accounts

Every entity must maintain an Entity Data Bank Administrator account. For security purposes, the Entity Data Bank Administrator account is limited to administrator functions only (cannot submit queries and reports). Entity Data Bank Administrators that also query and report must create a separate user account to do so. The Entity Data Bank Administrator account may only create, edit, delete, and update the passwords for other user accounts for the entity. Entities may have an unlimited number of additional user accounts.

To add or modify a user account, the Entity Data Bank Administrator selects **Maintain User Accounts** on the *Administrator Options* screen to display the *Maintain User Account* screen. Only the Entity Data Bank Administrator can access the *Maintain User Account* screen (Figure 2).
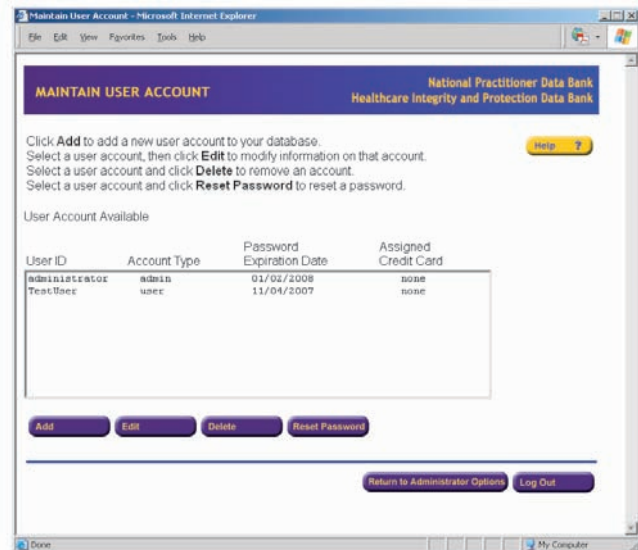

Figure 2. Maintain User Account Screen

To create a new user account, click **Add** on the *Maintain User Account* screen. The *User Account Information* screen displays, where the administrator may add information on a new user.

User IDs

All user IDs have the following characteristics:

- They must contain at least eight characters.
- They must contain only alphanumeric characters.

- They are case sensitive.
- They must be unique for the entity user.

To remove a user account, highlight the user's account information on the *Maintain User Account* screen and select **Delete**. The account is removed immediately.

To reset a user password, highlight the user's account information on the *Maintain User Account* screen, select **Reset Password**, and follow the on-screen instructions. Resetting a user's password will create a system generated temporary password that is valid for 3 calendar days. The user will be required to change the password upon the next IQRS login.

To edit a user account, highlight the user's account information on the *Maintain User Account* screen and click **Edit.** The *User Account Information* screen displays, where the Entity Data Bank Administrator may update the user's Name, Title, Telephone, E-mail, and Street Address. (Non-administrator users may also access the *User Account Information* screen and update their own account information by selecting **Update User Account** on the *Options* screen.)

User Passwords

Passwords must comply with the following requirements:

- They must contain at least eight characters.

- They must contain a combination of alphanumeric characters.

- They are case sensitive.

- They must contain at least one number.

- They must not contain a word found in the dictionary.

- They must not be your User ID.

- They must not be a common Data Bank phrase (e.g., NPDB, IQRS).

- They must not be a simplistic or systematic sequence (e.g., abcd1234).

Passwords may also include any of the following characters: **!@#$^&*( )-_=+[ ] { } | ;:,.< >?.**

Passwords are valid for 90 days. The expiration dates for all user passwords may be viewed by the Entity Data Bank Administrator on the *Maintain User Account* screen. After 90 days, users must change their passwords. The system will ensure that the new password is different from the previous four passwords used for that user ID. The system will prompt the user 5 days before the password expires. If the user does not change his or her password before it expires, one grace login will be provided, which can be used up to 30 calendar days after the password expiration. At the grace login, a warning message indicates that the password must be changed immediately; otherwise, the password will expire and future IQRS access will be denied.

IQRS Password Reset Service

To reset your expired Data Bank password without having to contact the Customer Service Center, you must have an e-mail address on file with the Data Banks and know your expired password. To reset your password, log in to the IQRS and click **Reset Password** on the *System Error* screen. An e-mail will be sent to the e-mail address specified in the IQRS user account and will contain a link which the entity must click to access the IQRS using their expired password. The user is then prompted to create a new password. **Note**: The new password link expires after one hour. Entities that do not complete the password reset process before the link expires will have to return to the IQRS to reset their password.

Procedures for Authorized Agents

Authorized Agent administrators may also create and maintain agent user accounts. The agent's administrator logs in to the IQRS. On the *Administrator Options* screen, click **Maintain User Accounts**. Select the **user ID** that you wish to update the querying and/or reporting privileges for and click **Edit**. On the *User Account Information* screen, the administrator can update user privileges by selecting the desired entities in the **Entities Available to Act on Behalf of** section and specifying whether the agent user can: Query Only, Report Only, Query & Report, or None. Be sure to click **Save** in order to save changes made on the *User Account Information* screen.

IQRS Security

The IQRS operates on a secure Web server and uses the latest technology, along with various implementation measures, to provide a secure environment for querying, reporting, data storage, and retrieval. Security features include the following:

- Firewall protection from unauthorized access.

- Encryption of transmitted data to prevent unauthorized use.

- Unique passwords for data entry and retrieval.

- Multiple unique user IDs to allow entities with multiple departments/people to use the same DBID for querying and reporting, overseen by a single administrator account that can add, update, or remove any of the user accounts.

- Encryption of transmitted data to prevent unauthorized use.

- Only one concurrent IQRS session permitted per user account.

- IQRS Entity Data Bank Administrator account limited to administrator functions only (cannot submit queries and reports).

NPDB-HIPDB Assistance

For additional information, visit the NPDB-HIPDB Web site at *www.npdb-hipdb.hrsa.gov*. If you need assistance, contact the NPDB-HIPDB Customer Service Center by e-mail at *help@npdb-hipdb.hrsa.gov* or by phone at 1-800-767-6732 (TDD 703-802-9395). Information Specialists are available to speak with you weekdays from 8:30 a.m. to 6:00 p.m. (5:30 p.m. on Fridays) Eastern Time. The NPDB-HIPDB Customer Service Center is closed on all Federal holidays.