



National Practitioner Data Bank Healthcare Integrity and Protection Data Bank



ENSURE INTEGRATED QUERYING AND REPORTING SERVICE (IQRS) SECURITY

There are over 17,000 registered entities with an average of three users per entity who access the Data Banks. Because of the high volume of users and sensitivity of information, the Data Banks require that entities take specific precautions to protect the confidentiality of information. Implementation of these specific measures can help prevent security breaches, which may result in civil suits and fines for violating Federal regulations under Title IV of Public Law 99-660, the *Health Care Quality Improvement Act of 1986*, Section 1128E of the *Social Security Act*, and other Federal statutes. To view Data Bank laws and regulations, see www.npdb-hipdb.hrsa.gov/legislation.html.

The Federal regulations specify Data Bank requirements for the confidential receipt, storage, and disclosure of information. Entity Data Bank Administrators are responsible for monitoring and controlling user access, which will help ensure the security of Data Bank information.

It is important to follow the best practices discussed below for creating secure passwords as well as entity users' access to the Data Banks. Equally important to the system's security is the proper and secure retrieval, handling, and disposal of sensitive Data Bank information.

1. IQRS SECURITY

The IQRS operates on a secure web server using the latest technology and implementation measures to provide a secure environment for querying, reporting, storing, and retrieving information.

2. DATA BANK CONFIDENTIALITY

Information reported to the Data Banks is considered confidential and may not be disclosed except as specified in the NPDB and HIPDB regulations.

To safeguard the system, the Data Banks require all entity accounts to have unique User IDs and User Passwords. This rule helps protect the confidentiality of Data Bank information. Each registered entity is assigned a Data Bank Identification Number (DBID), as well as a User ID, and User Password to be used by the individual the entity designates as the Entity Data Bank Administrator for that DBID account. The Entity Data Bank Administrator is required to assign a unique User ID and User Password to each additional entity employee that is authorized to query or report to the Data Banks. When logging in to the system, you must enter your password and other information to identify yourself to the Data Banks as an authorized user and, based on your entity's statutory authority and eligibility, you are granted the correct permissions to use the IQRS.

Please keep the following points in mind when using the IQRS:

- The Entity Data Bank Administrator and the individual user are responsible for protecting their user ids and passwords and preventing unauthorized access to Data Bank information. The first step to securing your account is a good password. See the "Formulate a Secure Password" section below for password specifics.
- The Entity Data Bank Administrator is responsible for maintaining the entity's account and the individual user accounts.

3. ENTITY DATA BANK ADMINISTRATOR RESPONSIBILITIES

The "Entity Data Bank Administrator" is the person assigned by your entity to oversee the use of the IQRS and to create and maintain individual user accounts for other staff. If more than one person in your organization submits queries and/or reports to the Data Banks, the Entity Data Bank Administrator must establish individual user accounts. The Entity Data Bank Administrator should never provide other users with the Entity Data Bank Administrator's login or password. To establish individual user accounts, the Entity Data Bank Administrator should log in to the IQRS, click **Administrator Options** on the *Entity Registration Confirmation* screen. Then, click **Maintain User Accounts** on the *Administrator Options* screen. On the *Maintain User Account* screen, the Entity Data Bank Administrator may add, edit, or delete individual user accounts and

specify a User ID and Temporary User Password for each user account established. See below for information on password security.

4. PASSWORDS

The Data Banks are mandated by Federal regulation to increase and scrutinize security in order to protect the confidential information stored in the Data Banks.

IQRS users are required to change their passwords every 90 calendar days. The user will receive an expiration notice 5 days prior to the expiration. After a password is expired, a user is granted 1 grace login up to 30 calendar days after the password expiration.

Resetting Passwords

If a user forgets his or her password or is locked out, the Entity Data Bank Administrator is responsible for resetting the password. The Entity Data Bank Administrator will create a system-generated, temporary password for the user. This password is valid for 3 calendar days. The user is required to change this password with their next login. There is no grace login once this temporary password expires.

If the Entity Data Bank Administrator forgets his or her password or is locked out, they must call the Customer Service Center at 1-800-767-6732 to reset the password. The Customer Service Center will create a system-generated, temporary password for the Entity Data Bank Administrator. This password is valid for 3 calendar days. The Entity Data Bank Administrator is required to change this password with their next login. There is no grace login once this temporary password expires.

Generated Passwords

Passwords mailed to new entities on entity registration confirmation documents are valid for 30 calendar days. The Entity Data Bank Administrator is required to change this password with their next login. There is no grace login once this temporary password expires.

Deleting User Accounts

The Entity Data Bank Administrator is responsible for updating user accounts. If a user leaves the organization, the Entity Data Bank Administrator must delete that person's user account.

5. FORMULATE A SECURE PASSWORD

Here are some tips for creating a secure password:

- Do not make your passwords easy to guess. Do not use any form of personal information (as-is, reversed, capitalized, etc.) such as your entity name, your name, the names of family members, your birthday, or the words NPDB or HIPDB.
- Use mixed-case passwords. User IDs and User Passwords are case sensitive and must contain at least eight (but no more than 14) characters, including at least one number and one letter.
- User Passwords (not User IDs) may also include any of the following special characters: !@#\$%^&*()-_=[] { } | ; : , < > ?
- Pick a phrase or question and use the first letter of each word, inserting a special character or two. For example, "Will It Rain Today?" could produce "W+i+r+t?04" as a password.
- Do not use a single word found in any dictionary, including foreign words. Make up nonsense words that are pronounceable, such as "bingzing3" or "zorpgorp11". Combine two short words with a special character, like "4truck+in" or "my2birds".
- Do not base your password on your User ID.

- Do not use a simplistic sequence (e.g., “abcd1234”) or base your password on an adjacent keyboard sequence (e.g., “qwertyuiop1”).
- In order to maintain password confidentiality, do not write down your password; remember it.

6. WHEN SECURITY IS COMPROMISED

Consider the following scenario: An Entity Data Bank Administrator shares his or her User ID and User Password with another user. That user accesses the Data Banks (using the Entity Data Bank Administrator’s log-on information) and, at the request of a practitioner, voids all active reports previously filed by the entity on the practitioner. In this scenario, both the practitioner and the user are liable and subject to civil money penalties (42 CFR Ch. V) and penalties under other Federal statutes. However, because the user entered the Entity Data Bank Administrator’s login and password to perform this unauthorized void transaction, the transaction will be traced to the Entity Data Bank Administrator. Avoid potentially disastrous situations by not sharing your login and password information.

7. OTHER SECURITY POINTERS

- Be sure to log out of the IQRS at the end of your session, so that unauthorized personnel cannot gain access to your sensitive information.
- After logging in to the IQRS, on the *Entity Registration Confirmation* screen, verify the date and time when your account was last accessed. If you notice that this date and time are incorrect, you should change your password immediately, call the Customer Service Center at 1-800-767-6732, and notify your Entity Data Bank Administrator.
- Remember that improper use of Data Bank information can result in a civil money penalty of up to \$11,000 per violation of confidentiality. By setting up passwords and using the system properly, you can help ensure IQRS security.
- Do not share confidential Data Bank documents with anyone who is not authorized to see them. Handle the reports properly – do not leave them out on printers or lying around the office. Securely store and file confidential documents.
- After a confidential Data Bank document is generated, print it and then immediately secure your files. Be sure to shred extra copies of documents that you do not intend to file.