ENSURE DATA BANK SECURITY

There are over 17,000 registered organizations with an average of three users per organization who access the Data Bank. Because of the high volume of users and sensitivity of information, the Data Bank requires that organizations 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 *http://www.npdb-hipdb.hrsa.gov/resources/aboutLegsAndRegs.jsp*.

The Federal regulations specify Data Bank requirements for the confidential receipt, storage, and disclosure of information. Each organization's Data Bank Administrator is 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 organization users' access to the Data Bank. Equally important to the system's security is the proper and secure retrieval, handling, and disposal of sensitive Data Bank information.

1. DATA BANK SECURITY

The Data Bank 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 Bank is considered confidential and may not be disclosed except as specified in the NPDB and HIPDB regulations.

To safeguard the system, the Data Bank requires all organization accounts to have unique user IDs and user passwords. This rule helps protect the confidentiality of Data Bank information. Each organization is assigned a Data Bank Identification Number (DBID) when they register with the Data Bank. In addition, the Data Bank Administrator must choose a user ID and password as part of the registration process. Once the registration is approved by the Data Bank, the Administrator can assign a user ID and password to each additional employee that is authorized to query or report to the Data Bank. When you sign in to the system, enter your password and other information to identify yourself to the Data Bank as an authorized user and, based on your entity's statutory authority and eligibility, you are granted the correct permissions to use the Data Bank.

Please keep the following points in mind when using the Data Bank:

- The 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 *http://www.npdb-hipdb.hrsa.gov/Passwords* for password specifics.

- The Data Bank Administrator is responsible for maintaining the organization's account and the individual user accounts.

3. DATA BANK ADMINISTRATOR RESPONSIBILITIES

The "Data Bank Administrator" is the person assigned by your organization to oversee the use of the Data Bank system 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 Bank, the Data Bank Administrator must establish individual user accounts. The Data Bank Administrator should never provide other users with the Data Bank Administrator's sign in information or password. To establish individual user accounts, the Data Bank Administrator should sign in to the Data Bank; click **Administrator Options** on the *Entity Registration Confirmation* page; then, click **Maintain User Accounts** on the *Administrator Options* page. On the *Maintain User Account* page, the 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 Bank is mandated by Federal regulation to increase and scrutinize security in order to protect the confidential information stored in the Data Bank.

Data Bank users are required to change their passwords periodically. Password restrictions and guidelines can be found at *http://www.npdb-hipdb.hrsa.gov/Passwords*.

Resetting Passwords

Every user has the ability to reset their password by using the Reset Password service. Click the **Forgot Your Password?** link on the *Data Bank Sign In* page. The user will enter their DBID and user ID and will be asked to answer one of the challenge questions that they previously set up. If the question is answered correctly, the user will be allowed to choose a new password, and an email will be sent that contains a link that allows them to sign into the Data Bank with their new password.

If the user is not eligible to reset their own password, because their account is locked or they have not set their challenge questions, the Data Bank Administrator will need to reset the password. The Data Bank Administrator will create a system-generated, temporary password for the user, which is valid for 3 calendar days. The user is required to change this password with their next sign in. There is no grace sign in once this temporary password expires.

If the organization Data Bank Administrator forgets his or her password or their account is locked, 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 Data Bank Administrator. This password is valid for 3 calendar days. The Data Bank Administrator is required to change this password with their next sign in. There is no grace sign in once this temporary password expires.

Generated Passwords

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

Deleting User Accounts

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

5. When Security is Compromised

Consider the following scenario: A Data Bank Administrator shares his or her user ID and user password with another user. That user accesses the Data Bank (using the Data Bank Administrator's sign in information) and, at the request of a practitioner, voids all active reports previously filed by the organization 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 Data Bank Administrator's sign in and password to perform this unauthorized void transaction, the transaction will be traced to the Data Bank Administrator. Avoid potentially disastrous situations by not sharing your sign in and password information.

6. Other Security Pointers

- Be sure to sign out of the Data Bank at the end of your session, so that unauthorized personnel cannot gain access to your sensitive information.
- After you sign in to the Data Bank, on the *Entity Registration Confirmation* page, 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 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 Data Bank 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.