



National Practitioner Data Bank Healthcare Integrity and Protection Data Bank



ENSURE REPORT RESPONSE SERVICE SECURITY

Federal regulations for the National Practitioner Data Bank and the Healthcare Integrity and Protection Data Bank specify requirements for the confidential receipt, storage, and disclosure of information, located at www.npdb-hipdb.hrsa.gov/legislation.html. When you use the Report Response Service, please follow the best practices discussed below for creating secure passwords and for retrieving, handling and disposing of sensitive documents.

1. REPORT RESPONSE SERVICE SECURITY

The Report Response Service operates on a secure web server using the latest technology and implementation measures to provide a secure environment for 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 protect the confidentiality of Data Bank information, the Data Banks assign a unique Report Number and initial Report Password to each report. When logging in to the Report Response System, please enter your Report Number and Report Password to identify yourself to the Data Banks.

3. PASSWORDS

The Data Banks are mandated by federal regulation to increase and scrutinize security. In order to protect the private information stored in the Data Banks, the password policies have been enhanced.

Expired Passwords

All Report Response Service 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 expiration. If the expired password is not reset within this time period, the user must contact the Customer Service Center at 1-800-767-6732 to reset the password (see Resetting Passwords below).

Resetting Passwords

If a subject forgets their Report Password or gets locked out of the Report Response Service, they must call the Customer Service Center at 1-800-767-6732 to reset the Report Password. The Customer Service Center will create a temporary password for the user. This password is valid for 3 calendar days. The subject is required to change this password with their next login. There is no grace login once this temporary password expires.

Generated Passwords

Passwords mailed on subject notification documents and self-query responses are valid for 30 calendar days. A Report Password can be found in the Report Response Service Login Instructions contained within the subject notification document. The subject is required to change this password with their next login. There is no grace login once this temporary password expires. **Note:** If a subject already established a valid Report Password in the Report Response Service, the subject notification document may not contain a Report Password and will instead direct the subject to use their previously established password when logging in to the Report Response Service.

4. 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 (as-is, reversed, capitalized, etc.) of personal information: e.g., your name, the names of family members, your birthday, or NPDB.
- Use mixed-case passwords. Report Passwords are case sensitive and must contain at least eight (but no more than 14) alphanumeric characters (they must contain at least one number and one letter).
- Report Passwords 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 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.

5. OTHER SECURITY POINTERS

- Be sure to log out of the Report Response Service at the end of your session, so that unauthorized persons cannot gain access to your sensitive information.
- 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 Report Response Service security.
- Handle the reports properly – do not leave them out on printers or lying around the office. Securely store and file reports.