



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 <http://www.npdb-hipdb.hrsa.gov/resources/aboutLegsAndRegs.jsp>. 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 Bank 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, a unique Report Number and initial Report Password is assigned to each report. When signing in to the Report Response System, please enter your Report Number and Report Password for identification purposes.

3. PASSWORDS

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

Expired Passwords

All Report Response Service 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

If a practitioner forgets their Report Password or if their account is locked, 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 practitioner is required to change this password with their next sign in. There is no grace sign in once this temporary password expires.



National Practitioner Data Bank Healthcare Integrity and Protection Data Bank



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 Sign In Instructions contained within the subject notification document. The practitioner is required to change this password with their next sign in. There is no grace sign in once this temporary password expires. **Note:** If a practitioner 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 practitioner to use their previously established password when signing in to the Report Response Service.

4. OTHER SECURITY POINTERS

- Be sure to sign 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.