Data Bank Administrator
Handbook

CONTENTS

Overview

Starting on January 24, 2011, the National Practitioner Data Bank-Healthcare Integrity and Protection Data Bank (NPDB-HIPDB) will require all individuals requesting a Data Bank account to complete a registration process which includes establishing their identity. This requirement applies both to new first-time users and to established users at organizations that are already registered. Existing users will be identity-proofed as part of their organization's first registration renewal after February 23, 2011.

How does the Data Bank verify each registrant's identity? That's where the Data Bank Administrator comes in. The Administrator acts as a representative of the Data Bank by confirming the identity and employment of each employee of the Administrator's organization who requests an NPDB-HIPDB account. Data Bank Administrators receive special Administrator Training in order to be able to perform the identity verification functions connected with Data Bank user registration and renewal.

Primary Responsibilities

Administrators act on behalf of the Data Bank to create user accounts and confirm the identity of each employee of the Administrator's organization who requests a Data Bank user account. Their primary responsibilities include the following vital functions:

- Create new user accounts.
- Verify the identity and employment status of each prospective user prior to the issuance of an account.
- Activate user accounts.
- Ensure that users' registration paperwork is completed accurately and on time.
- Submit users' registration paperwork by mail to the Data Bank.

The above functions can only be performed by Data Bank Administrators who complete the new Data Bank Administrator Training, which is available on the *Administrator Options* page of the Data Bank Web site. Some administrative functions, such as deleting user accounts and renewing an organization's registration, do not require Administrator Training.

Data Bank User Accounts

The Data Bank Administrator will approve and create new user accounts, and in connection with registration renewals will select which of the organization’s current users will retain their Data Bank accounts. Data Bank account holders may be any of the following:

- Organization user – An individual employed by the Administrator’s organization who is authorized by that organization to submit reports or queries to the NPDB, HIPDB, or both. There is no limit to the number of user accounts an organization may request to perform its Data Bank transactions (reporting, querying, and billing functions).
- Data Bank Administrator – An employee assigned to perform Administrator functions for the organization. Organizations may assign multiple Data Bank Administrators. This allows for administrative responsibilities to be divided or shared among multiple personnel; allows for an administrative backup; and allows departing Administrators to designate a replacement.

Note that Administrator accounts will have the ability to query and report, so there is no need to have separate accounts for individuals who function as both user and Administrator.

The Registration Process

The user registration process begins when the Administrator creates a new user account or specifies that an existing user account is to be retained. This is performed in the *Maintain User Accounts* section of the Data Bank Web site. The process involves a number of coordinated steps on the part of the registrant and the Data Bank Administrator.

1. As soon as the Administrator submits a new user or renewal request, the registrant will receive an email instructing him or her how to proceed. Renewing users will be required to sign in to the Data Bank to confirm their contact information. New registrants will find a link to a *User Account Request* Web page where they can enter their contact information, establish their own passwords, and set their notification preferences.
2. Both renewing users and new registrants will print one of two versions of the Registration document, depending on their geographic proximity to their organization's Administrator. If a registrants can be identity-proofed by their Administrator, they will download the "Verify With Your Data Bank Administrator" version; if they elect instead to have their identity verified by a Notary Public, they will download "Verify With a Notary Public" version.
3. The Administrator will be notified by email when the Registration document has been downloaded, as a means of letting him or her know where the user is in the registration process.
4. The Registration document contains identity verification instructions to the user. This process is called identity-proofing, and may be performed either by the Data Bank Administrator or by a Notary Public, who records the proof of identity on the Registration document. Registrants who have their identity verification performed by a Data Bank Administrator must show the Administrator these items:
    - Their unsigned NPDB-HIPDB User Registration document.
    - A non-expired photo identification (valid identification documents are discussed in the next section).

    Registrants who use a Notary Public for identity verification must present:
    - Their unsigned NPDB-HIPDB User Registration document.
    - A non-expired Government-issued photo ID (acceptable forms of identification are discussed in the next section).

The Registration Process (Continued)

5. In cases where the Administrator performs the identity-proofing, he or she will retain the completed, verified Registration document. If the prospective user was identity-proofed by a Notary Public, then the user must send the **original document** to his Data Bank Administrator (via interoffice mail or postal mail, for example).
6. The Administrator will review the Registration document and either approve or reject the registration request based upon criteria which are discussed later in this Handbook (see page 7). Existing users who complete the identity-proofing process as part of their organization's registration renewal will retain their accounts and be able to continue using the Data Bank for the duration of the registration process. For new registrants, the Data Bank Administrator will have to sign in to the Data Bank to activate (or reject) the user account. This is a temporary approval, contingent upon the Data Bank receiving the Registration documents within 15 days and other criteria.
7. For new users who are approved, the Administrator must communicate the organization's Data Bank Identification Number (DBID) to the user verbally (i.e., in person or via phone). The user will need the DBID, in addition to his username and password, to sign in to the Data Bank. New users will also receive a confirmation email from the system with further instructions.
8. Finally, the Administrator must mail the user's original, signed Registration document to the Data Bank within 15 days of approval. User accounts will be deactivated if the documents are not received within this time frame. The Data Bank will perform its own review of the document and confer final approval if it finds no problems. Administrators will receive notification only if the Data Bank rejects the account.
9. In cases where Administrators reject a registration request, they should destroy the Registration document.

Valid Identification Documents

Users or prospective users who use their Administrator for identity-proofing must present one of the following forms of photo identification:

- **Work Badge**
  An unexpired photo ID badge, such as a work badge, that is issued by the registered organization and that indicates the user's affiliation to the organization. In addition to a photo, the work badge must have all of the following: a serial number, the name of the organization, and an expiration date.
- **Government-Issued Photo ID**
  If a work badge is not available or does not have the required information, an alternate form of ID is required which establishes the user's identity. It must be an unexpired Government-issued photo ID that includes a serial number, such as:
  - Driver's license
  - Passport from country of citizenship, issued by Federal, State or local Government agency (must have name, date of birth, gender, height, eye color and address)
  - U.S. Military ID
  - Certificate of U.S. Citizenship
  - Certificate of Naturalization
  - Permanent or unexpired temporary resident card
  - Native American tribal document

Users who have their identities verified by a Notary Public should produce a Government-issued photo ID conforming with the previous section of this handbook.

The Fine Points of Identity-Proofing

Identity-proofing normally takes place when an organization is establishing new user accounts or during an organization's registration renewal process. It may also take place when existing users have a name change, in which case they are required to update their user account and print a new Registration document.

When users present themselves to the Administrator for identity-proofing, the Administrator should evaluate the following:

- Is the user presenting the proper type of ID?
- Does the ID have all of the required information? (see *Valid Identification Documents* on page 7)
- Is the expiration date on the ID later than today?
- Is the photo a reasonable likeness of the person standing before you? If you are skeptical that the photo on the ID represents the person standing before you, you should reject the registration request.
- Does the ID appear tampered with? If so, you should reject the registration request.
- Does the name on the ID match the name on the Registration document? In some cases, there may be variances, such as when a shortened or familiar version of the legal name is used on the work badge. If the name variance is enough to cause uncertainty about the user's identity, you should ask for a second form of photo ID.
- Is the user a current employee of the organization or agent? If the user's organizational affiliation cannot be verified, the request should be rejected.

Failure to meet any of the above criteria is cause for rejecting the registration request. If all of the above criteria are met, the Data Bank Administrator can approve the user's registration. The Administrator should witness the registrant's signature and then sign and date the document. If the registrant has already signed the Registration document, have them draw a single line through the signature, initial the change, and re-sign and date the document.

The Fine Points of Identity-Proofing (Continued)

The Data Bank Administrator must ask different questions if the Registration documents are signed by a Notary Public. In this situation, the Data Bank Administrator should consider the following:

- Is the Registration document an original document—not a copy or facsimile?
- Is the Registration document complete, clearly identifying the individual submitting it?
- Is the Registration document signed by both the user and the Notary Public?
- Do the signature dates of the Notary and the user match?
- Was the proper type of ID presented (as recorded on the Registration document)?
- Did the Notary complete the "Notary Public use only" section of the Registration document and provide an official notary seal or stamp?
- Is the user a current employee of the organization or agent?

A Registration document that does not meet all of the above criteria must be rejected.

Deleting User Accounts

There are a variety of reasons for deleting a user account. Examples would include but not be limited to: the user is no longer affiliated with the organization, or the user no longer has a need to use the Data Bank. In addition, it is necessary to delete a user account when:

- The account has been compromised (e.g., a user's sign-in information has been stolen).
- The account user has violated the NPDB-HIPDB Rules of Behavior which he or she agreed to upon first signing in to the account.
- The account was subjected to unauthorized use (e.g., the user's sign-in information was shared with a co-worker).
- For any other reason that a Data Bank Administrator deems a security risk.

In addition, the Data Bank will disable a user's account when it has been inactive for a period of 3 years.

Administrators may delete user accounts as necessary through the Web site's *Maintain User Accounts* page; this function may be performed by any Administrator, not only those who have completed the Administrator Training. If the Data Bank Administrator or the Data Bank Web site is unavailable for performing this function when needed, the user or Administrator should contact the NPDB-HIPDB Customer Service Center at 800-767-6732.