NATIONAL PRACTITIONER DATA BANK - HEALTHCARE INTEGRITY AND PROTECTION DATA BANK (NPDB-HIPDB)

Registration Practices Statement

Version 1.00

June 2010

Contract Number 263-01-D-0050
Task Order HHSH230G5004

CM Number NPDB- 04443.01.00

Submitted To:

U.S. Department of Health and Human Services
Health Resources and Services Administration
Bureau of Health Professions
Division of Practitioner Data Banks
Parklawn Building, Room 8-103
5600 Fishers Lane
Rockville, Maryland 20857

Prepared by:

SRA International, Inc.
4350 Fair Lakes Court
Fairfax, Virginia 22033-4233

DISCLOSURE STATEMENT

Table of Contents

List of Tables

1.0 Executive Summary

In accordance with federal guidelines for securing the National Practitioner Data Bank-Healthcare Integrity and Protection Data Bank (NPDB-HIPDB) system against unauthorized use, the Data Banks have established a Registration Practices Management body that is responsible for the identification and authentication of all NPDB-HIPDB users who have electronic access to the system. A Registration Practices Statement (RPS) describes the practices that the Registration Practices Management body employs for authenticating the identity of its users to issue accounts or credentials[1] that provide system access, as well as managing or revoking accounts in accordance with specific requirements.

This RPS describes the roles and responsibilities of all NPDB-HIPDB participants as they pertain to registration, details the identity proofing and registrations practices implemented by the Registration Practices Management body for each system user (i.e., role), identifies account life cycle operational requirements, references where information on facility, management, operational and technical security controls may be found, stipulates when the registration practices in this document must be reviewed and covers other business and legal considerations. Note that registration processes and sample registration forms are not included in this document; that information may be found in the *Registration Practices Management Operations Manual*.

The target audience for the RPS includes NPDB-HIPDB authorities such as its e-Authentication Manager and Change Control Board (CCB) and all other personnel fulfilling roles within the Registration Practices Management body; therefore, this RPS is considered an internal document.

[1] Except where otherwise specifically noted, all references in this RPS to "Accounts" or "Credentials" shall mean NPDB-HIPDB accounts for accessing the NPDB-HIPDB system.

2.0 Registration Practices Overview

The remainder of this introductory section describes the registration policy guidelines that are followed by this RPS, the scope of this document, NPDB-HIPDB's registration roles and responsibilities, and the administration responsibilities for this RPS.

2.1 Registration Policy

This document follows the guidelines provided for Level 2 and Level 3 (for the Investigative Search interface only) assurance level rating requirements stipulated in *E-Authentication Guidance for Federal Agencies* (OMB M-04-04) and the National Institute of Standards and Technology's (NIST) Draft Special Publication 800-63-1, *Electronic Authentication Guidelines*, and the recommendations of the *National Practitioner Data Bank-Healthcare Integrity and Protection Data Bank (NPDB-HIPDB) E-Authentication Requirements Analysis – December 2008*, CM# NPDB- 04443.01.00 [NPDB EAUTH]).

2.2 Scope

The structure of this RPS is based on "best practices" documentation developed for the Federal Government and commercial industry to describe the rigorous registration practices for Public Key Infrastructure (PKI) systems. This RPS describes the practices followed by NPDB-HIPDB to identify users, and to issue, manage and revoke credentials for accessing the NPDB-HIPDB system.

2.3 NPDB-HIPDB Participant Roles and Responsibilities

2.3.1 NPDB-HIPDB Authorities

There are four distinct entity categories within the NPDB-HIPDB community. As shown here, each category includes several roles. The roles within each category are described in the following sections of this document:

Registration Practices Management

- Division of Practitioner Databanks (DPDB) e-Authentication Manager
- NPDB-HIPDB Change Control Board (CCB)

Trusted Operations

- NPDB-HIPDB Customer Service Center/Document Control Center Operator
- NPDB-HIPDB System Administrators
- NPDB-HIPDB Information System Security Officer (ISSO)

User Administration

- Entity/Agency Certifying Official
- Entity Data Bank Administrator
- Authorized Agent Data Bank Administrator

End Entities

- Entity User
- Authorized Agent
- Investigator
- Self-Querier
- Report Subject

2.3.1.1 Registration Practices Management

2.3.1.1.1 DPDB e-Authentication Manager

The DPDB e-Authentication Manager manages and administers all e-Authentication efforts for NPDB-HIPDB within HRSA. The DPDB e-Authentication Manager has technical oversight and is responsible for NPDB-HIPDB, and participates on the NPDB-HIPDB Configuration Control Board.

2.3.1.1.2 NPDB-HIPDB Change Control Board (CCB)

The NPDB-HIPDB CCB is responsible for creating, maintaining and implementing this RPS and all registration practices and procedures regarding the NPDB-HIPDB System.

2.3.1.2 Trusted Operations

2.3.1.2.1 NPDB-HIPDB Customer Service Center/Document Control Center Operator(s)

The individual(s) responsible for processing registration documentation, disseminating Administrator account information (e.g., DBID, User ID, password) for new accounts, completing a self-query request, looking up billing information, etc.

2.3.1.2.2 NPDB-HIPDB System Administrator

The individual(s) responsible for creating Windows, Unix, and database accounts that provide system operators (e.g., customer service representatives) with access to physical machines and applications; each has varying roles and access permissions.

2.3.1.2.3 NPDB-HIPDB Information System Security Officer (ISSO)

The ISSO creates and maintains the security policy, roles, and other applicable information that is used within the NPDB-HIPDB regarding access control.

2.3.1.3 User Administration

2.3.1.3.1 Entity/Agency Certifying Official

The individual selected and empowered by an entity to certify the legitimacy of a registration for participation in the NPDB-HIPDB.

2.3.1.3.2 Entity Data Bank Administrator

The Entity Data Bank Administrator sponsors, approves, revokes and assigns privileges (e.g., query, report or both) to Entity Users. The Entity Data Bank Administrator may also designate an Authorized Agent (organization) to submit reports and queries on the Entity's behalf.

2.3.1.3.3 Authorized Agent Data Bank Administrator

The Authorized Agent Data Bank Administrator sponsors, approves, revokes and assigns privileges (e.g., query, report or both) to Authorized Agents (Users).

2.3.1.4 End Entities

2.3.1.4.1 Entity User

An individual authorized by an Entity to submit a report and/or query to the NPDB, HIPDB, or both. Entities may maintain an unlimited number of user accounts to submit transactions (e.g., queries, reports) and retrieve responses from the Data Banks.

2.3.1.4.2 Authorized Agent (User)

An employee of an Authorized Agent organization with a user account that may query and/or report on behalf of an Entity. This user role's functions are identical to that of an Entity User.

2.3.1.4.3 Self-Querier

An individual health care practitioner (e.g., licensed physician, dentist, audiologist, clinical social workers), provider or supplier who may query the NPDB-HIPDB for information about themselves or the organization they work for. A self-querier may also be a report subject (described below).

2.3.1.4.4 Report Subject

An individual or organization that is the subject of a Medical Malpractice Payment Report, an Adverse Action Report, or a Judgment or Conviction Report. When a report is submitted to NPDB-HIPDB, the Data Banks processes the report and sends a Report Verification Document, including a copy of the report, to the reporting entity. A Notification of a Report in the Data Bank(s), which includes a copy of the report, is also sent to the report subject. The entity that filed a report may change the information in the report; a report subject cannot change the information in the report, but may supplement using the NPDB-HIPDB website to add a Subject Statement and/or dispute the report. A report subject may also request the report be elevated to secretarial review. A dispute and secretarial review request may regard the accuracy of the report, whether or not it was submitted according to NPDB-HIPDB reporting requirements, or the eligibility of the entity to report the information. A report subject may also self-query (described above).

2.3.1.4.5 Investigator

Federal and State law enforcement agencies (registered as an Entity) submit report data (e.g., criminal convictions and civil judgments against health care practitioners, providers and suppliers related to health care) to the HIPDB as well as query the HIPDB using the Investigative Search Capability (ISC). By providing an Originating Reporting Agency Identifier (ORI) number at the time of registration, law enforcement agency investigators may perform free text ad hoc queries against the HIPDB. Federal and State law enforcement agencies also can submit explicit queries to the NPDB.

2.3.2 Relying Parties

The right to rely reasonably on a NPDB-HIPDB Credential is limited to the NPDB-HIPDB System.

2.3.3 Auditors

The DPDB e-Authentication Manager or the NPDB-HIPDB CCB can initiate an audit of NPDB-HIPDB Entity and Authorized Agent organizations to determine compliance with the registration practices described in this document.

2.4 RPS Administration

2.4.1 Specification of Administration Organization

The NPDB-HIPDB CCB is responsible for all aspects of this RPS.

2.4.2 Contact Person for this RPS

The contact person for this RPS shall be the DPDB e-Authentication Manager. Questions regarding this document should be directed to the DPDB e-Authentication Manager through the NPDB-HIPDB Document Control Center at the following address:

National Practitioner Data Bank - Health Care Integrity and Protection Data Bank

P.O. Box 10832

Chantilly, Virginia 20153-0832

2.4.3 Person Determining RPS Suitability

The NPDB-HIPDB CCB is responsible for determining the suitability of this RPS.

2.4.4 RPS Approval Procedures

The NPDB-HIPDB CCB is responsible for approving this RPS as it relates to implementing the specific registration practices.

3.0 General Provisions

Rights and Obligations

3.1.1.1 Registration Practices Management Obligations

3.1.1.1.1 DPDB e-Authentication Manager Obligations

The DPDB e-Authentication Manager has the following obligations:

- Provide e-Authentication oversight for NPDB-HIPDB.
- Request revocation of Entity/Agent Databank Administrator, Entity/Authorized Agent User, Investigative Search User and Self-Querier accounts to the NPDB-HIPDB Customer Service Center as needed.
- Approve creation of emergency accounts.

3.1.1.1.2 NPDB-HIPDB CCB Obligations

The NPDB-HIPDB CCB shall ensure that the NPDB-HIPDB registration practices are operating in accordance with this RPS.

3.1.1.2 Trusted Operations Obligations

3.1.1.2.1 NPDB-HIPDB Customer Service Center/ Document Control Center Operator Obligations

NPDB-HIPDB Customer Service Center/Document Control Center Operators have the following obligations:

- Verifying the accuracy of information entered in the Entity/Authorized Agent registration package.
- Process incoming registration documents for registering Certifying Officials, Data Bank Administrators, Entity/Authorized Agent users, self-queriers and Investigative Search users.
- Approve and forward registration documents for archival after successfully verifying the information.
- Scan and archive all registration documents.
- Provide customer service support to the NPDB-HIPDB System users.
- Issue tokens to Investigative Search users and manage the token process.
- Provide account setup information to the Entity/Agent Data Bank Administrator.

3.1.1.2.2 NPDB-HIPDB System Administrator Obligations

NPDB-HIPDB Administrators are obligated to maintain the NPDB-HIPDB systems and technical infrastructure, which includes:

- Perform backups and recovery for the NPDB-HIPDB software, data, and logs;
- Monitoring of the software application platform and reporting of non-working services;
- Performance of the operation and maintenance of the hardware and operating systems;

- Execution of scripts and routines that manage the NPDB-HIPDB systems;
- Creating Customer Service Center Operation system accounts;
- Initiating change control procedures to perform upgrades or install patches.

3.1.1.2.3 NPDB-HIPDB ISSO Obligations

The ISSO has the following obligations:

- Designate all policy settings for the NPDB-HIPDB System in accordance with the NPDB-HIPDB policies and this RPS.
- Provide guidance for registering Data Bank administrators and users when notified of emergency situations.

3.1.1.3 User Administration

3.1.1.3.1 Entity/Authorized Agent Certifying Official Obligations

An Entity/Authorized Agent's Certifying Official has the following obligations:

- Submit correct information in the registration documentation.
- Request to revoke the Entity/Authorized Agent Data Bank Administrator's account if there is a danger of it being compromised or subjected to unauthorized use in any way, or if any information affecting the reliability of the account changes or is no longer true (e.g., name changes, no longer employed, associated or affiliated with the Organization).

3.1.1.3.2 Entity Data Bank Administrator Obligations

Entity Data Bank Administrators have the following obligations:

- Submit correct information in the registration documentation.
- Protect the NPDB-HIPDB account (e.g., safeguard login credentials, log in from a secure location).
- Request to revoke their own account if there is a risk of it being compromised or subjected to unauthorized use in any way, or if any information affecting the reliability of the account changes or is no longer true (e.g., name changes, no longer employed, associated or affiliated with the Organization).
- Successfully complete training in identity proofing procedures for Entity Users.
- Identity proof Entity Users by following the registration practices described in this document and approve the issuance of the NPDB-HIPDB credentials.
- Revoke Entity User Accounts upon request from Entity Users or if there is a risk of it being compromised or subjected to unauthorized use in any way, or if any information affecting the reliability of the account changes or is no longer true (e.g., name changes, no longer employed, associated or affiliated with the Organization).

3.1.1.3.3 Authorized Agent Data Bank Administrator Obligations

Authorized Agent Data Bank Administrators have the following obligations:

- Submit correct information in the registration document.

- Protect the NPDB-HIPDB account (e.g., safeguard login credentials, log in from a secure location).
- Successfully complete training in the identity proofing procedures of Authorized Agents.
- Identity proof Authorized Agents by following the registration practices described in this document and approve the issuance of the NPDB-HIPDB credentials.
- Request to revoke their own account if there is a risk of it being compromised or subjected to unauthorized use in any way, or if any information affecting the reliability of the account changes or is no longer true (e.g., name changes, no longer employed, associated or affiliated with the Organization).
- Revoke Authorized Agent Accounts upon request from Authorized Agents or if there is a risk of it being compromised or subjected to unauthorized use in any way, or if any information affecting the reliability of the account changes or is no longer true (e.g., name changes, no longer employed, associated or affiliated with the Organization).

3.1.1.4 End Entities Obligations

3.1.1.4.1 Entity User Obligations

The Entity Users have the following obligations:

- Submit correct information in the registration document.
- Protect the NPDB-HIPDB account (e.g., safeguard login credentials, log in from a secure location).
- Request to revoke the account if there is a risk of it being compromised or subjected to unauthorized use in any way, or if any information affecting the reliability of the account changes or is no longer true (e.g., name changes, no longer employed, associated or affiliated with the Organization).

3.1.1.4.2 Authorized Agent (User) Obligations

The Authorized Agent (User) has the following obligations:

- Submit correct information in the registration document.
- Protect the NPDB-HIPDB account (e.g., safeguard login credentials, log in from a secure location).
- Request to revoke the account if there is a risk of it being compromised or subjected to unauthorized use in any way, or if any information affecting the reliability of the account changes or is no longer true (e.g., name changes, no longer employed, associated or affiliated with the Organization).

3.1.1.4.3 Self-Querier Obligations

The Self-Querier has the following obligations:

- Submit the correct information in the individual and organizational self-query registration documents.
- Protect the NPDB-HIPDB account (e.g., safeguard login credentials, log in from a secure location).

- Request to revoke the account if there is a risk of it being compromised or subjected to unauthorized use in any way.

3.1.1.4.4 Report Subject Obligations

The Report Subject has the following obligations:

- Protect the NPDB-HIPDB account (e.g., safeguard login credentials, log in from a secure location).
- Request to revoke the account if there is a risk of it being compromised or subjected to unauthorized use in any way.

3.1.1.4.5 Investigative Search Obligations

Investigative Search users have the following obligations:

- Submit correct information in the registration document.
- Protect the NPDB-HIPDB account and token (e.g., safeguard login credentials, log in from a secure location).
- Request to revoke the account if there is a risk of it being compromised or subjected to unauthorized use in any way, or if any information affecting the reliability of the account changes or is no longer true (e.g., name changes, no longer employed, associated or affiliated with the Organization).

Liability

3.1.2 NPDB-HIPDB Liability

NPDB-HIPDB accounts are issued to further the mission and operations of NPDB-HIPDB, HRSA and HHS and liability claims shall be subject to the terms of the federal tort claims act as interpreted by the HHS Office of General Counsel.

3.1.3 End-User Liability

The users of the NPDB-HIPDB System are solely responsible for meeting their obligations per a Subscriber Agreement presented to them upon initial login to their account. A sample Subscriber Agreement can be found in the *Registration Practices Management Operations Manual*. Failure of the users to comply with the Subscriber Agreement is grounds for NPDB-HIPDB credential revocation. The users waive any and all claims against the Service, its agents and employees, contractors and assignees for any action arising from the use or possession of NPDB-HIPDB credentials.

4.0 Identification and Authentication

4.1 Initial Entity Registration

As described in *National Practitioner Data Bank-Healthcare Integrity and Protection Data Bank (NPDB-HIPDB) Identity Proofing and Registration Process Alternatives-June 2009,* DCN 12313-114-101-NPDB-IDP-REG-20090630 [NPDB-IDPROOF] document, the initial Entity registration consists of three steps that represent the process of downloading, completing and submitting registration documentation.

4.1.1 Authentication of Entity Identity

The *Entity Registration* document includes the Entity's Name, Address and Federal Tax Identification Number (TIN). The NPDB-HIPDB Customer Service Operator shall authenticate this information through record checks through applicable agencies or third party service providers to verify the information provided in the registration document is accurate.

4.1.2 Authentication of the Certifying Official and Entity Data Bank Administrator Identities

The Certifying Official and Entity Data Bank Administrator provide valid identification to a notary public as a part of Entity registration. An overview of the entire process is as follows:

a) The Data Bank Administrator visits the online Entity Registration service and begins the registration process. The user fills out the registration document online, establishes an Administrator user ID and password, and is issued a Data Bank Identification (DBID) number. The user prints out the *Entity Registration* document *w*ith the provided information pre-populated. Both the Certifying Official's and the Data Bank Administrator's registration documents are a part of this printout.

b) As part of the Entity Registration process, the Certifying Official and Entity Data Bank Administrator must provide two forms of ID and sign separate registration documents in front of a notary (U.S.-based Entities located in countries outside of the United States may utilize notary services available at the local US Consulate[2]). The notary shall record the Certifying Official and Entity Data Bank Administrator's personal information (identification number, expiration date) from the IDs presented onto the registration document. One form of identification must be a valid State or Federal government-issued photo ID.

   Forms of acceptable ID are as follows: An unexpired state-issued photo ID (with a serial number) such as a driver's license; Passport from country of citizenship, federal, state or local government agency (must have name, date of birth, gender, height, eye color and address); US military ID; Certificate of U.S. Citizenship; Certificate of Naturalization; permanent or unexpired temporary resident card; Native American tribal document; or Canadian driver's license.

c) The notary shall complete a separate section describing their certification (e.g., state/county in which they operate) and sign a statement acknowledging that the Certifying Official and Entity Data Bank Administrator appeared in front of them and for what purpose, date the document and provide a notary stamp or seal.

d) The Entity, Certifying Official and Data Bank Administrator forms may be combined into one registration package and mailed to the NPDB-HIPDB, or if the Certifying Official and the Data Bank Administrator are in different locations, the registration documents may be sent separately to the NPDB-HIPDB.

[2] Practice Note: For locations outside the US, where such notary services are unavailable, the self-certified registration documents may be sent to NPDB-HIPDB ISSO for approval.

4.1.3 Authentication of the Affiliation of the Certifying Official and Entity Data Bank Administrator to the Registering Entity

This is established by one of the following methods:

- **Option 1 -** The Certifying Official and Entity Data Bank Administrator presents an unexpired photo ID badge issued by the registering Entity that indicates their affiliation to the Entity (work badge) along with the notarized registration document. The notary shall record on the document that the photo ID badge issued by the Entity was presented. A photocopy of the Certifying Official and Entity Data Bank Administrator badges will be sent along with the individual's notarized registration document.
- **Option 2 -** The Certifying Official and Entity Data Bank Administrator may provide a signed letter on company letterhead from an authorized organization official (e.g., a person from Human Resources or Payroll) attesting to the affiliation. A permitted exception would be an authorization letter from a one-person company as long as the company's information can be verified by NPDB-HIPDB Operations.

Once the Entity's registration package is approved by NPDB-HIPDB, a *Registration Verification* notice shall be emailed to the Entity Data Bank Administrator as per current practice. Upon receipt, the Entity Data Bank Administrator completes the registration by logging in using the credentials supplied during the initial online registration process.

4.2 Initial Authorized Agent Registration

This process is the same as the Entity Registration process described above in Section 3.1.

4.3 Initial Entity User Registration

The Entity Data Bank Administrator completes an online request to begin the process of creating a user account (information required by the online *User Account Request* page will be minimal, such as User Name, User Login ID, Contact Information and Email Address, and an optional confidential pass phrase).

The user receives an email with a link to a registration page. The user completes the *User Registration* page online, specifies a password, prints out the resulting document and takes it to the Entity Data Bank Administrator (or if remotely located, a notary).

The Entity Data Bank Administrator or notary will (a) ensure authentication of the Entity User identity and (b) ensure affiliation of the Entity User to the Registering Entity by identity proofing the user as listed in the table below.

Table 1: Identity Proofing an Entity User

Entity Data Bank Administrator	Notary*
■ Reviews and records personal information from the Entity User's work badge, AND/OR ■ Checks Entity enterprise records to verify employment of the Entity User.	■ Records the information from a valid State or Federal government-issued photo ID. Forms of acceptable ID are as follows: A state-issued photo ID (with a serial number) such as a driver's license; Passport from country of citizenship, federal, state or local government agency (must have name, date of birth, gender, height, eye color and address); US military ID; Certificate of U.S. Citizenship; Certificate of Naturalization; permanent or unexpired temporary resident card; Native American tribal document; AND ■ Reviews work badge with photo ID OR reviews and confirms signed letter on company letterhead from an authorized organization official attesting to the affiliation was provided by the Entity User.

* If available.

If the user's identification is valid, the user shall sign and date the *User Registration* document in front of the Entity Data Bank Administrator (or Notary) who will also sign and date it. The Entity Data Bank Administrator sends the signed document to the Data Banks via mail for archive purposes. For the account to remain active, the signed registration document must be received no later than 30 days from the time the Data Bank Administrator approves creation of the account.

The Entity Data Bank Administrator approves the creation of the account using the IQRS interface and the account is activated. As a result of approval, the user will receive an approval email and can access the NPDB-HPDB System.

NOTE: To handle cases where the Data Bank Administrator is also a user (e.g., in small hospitals), the Data Bank Administrator will automatically be given user privileges upon successful registration.

For access to the NPDB-HIPDB through ITP and QRXS interfaces, it is assumed that the client system will have an owner/sponsor and the Entity Data Bank Administrator will identity proof the owner/sponsor with the same process.

4.4 Initial Authorized Agent User Registration

This process is the same as the Entity User Registration process described above in Section 3.3.

4.5 Initial Investigative Search User Registration

Investigative Search users complete an *Investigative Search User Registration* document and submit the notarized document to the NPDB-HIPDB Document Control Center for review and approval. Approval requires verification of the Investigative Search user's employment, which can be done by contacting the agency's Human Resources Department.

If the NPDB-HIPDB Document Control Center Operator approves the registration, the Investigative Search user shall be sent a two-factor authentication token along with instructions for logging into the system.

4.6 Initial Self-Querier Registration

The Self-Querier submits a notarized *Self-Querier Registration* document that contains information from an ID issued by the Federal or State Government (e.g., driver's license, passport) such as serial number, expiration date, address and credit card information for either him/herself or his/her organization. The self-query report is generated and sent back to the address specified in the document or may be accessed electronically.

4.7 Initial Report Subject Registration

NPDB-HIPDB Document Control Center Operations forwards to the Report Subject via postal mail the report along with a report number and password to access the information online. Personally Identifiable Information (PII) data is considered sensitive and therefore shall be masked (i.e., the original data is hidden or filtered) in the printed report.

4.8 Trusted Operator Accounts

Trusted Operator accounts are created as specified in the NPDB-HIPDB System Security Plan.

4.9 Account Renewal and Update

4.9.1 Account Renewal

Entities are required to renew their NPDB-HIPDB accounts every two years starting from the date of approval of their initial registration. Data Bank Administrators may renew the Entity/Agent Registration, the Entity/Agent User registrations and Investigative Search User registrations through use of current NPDB-HIPDB credentials. As part of the renewal process, Data Bank Administrators will be given the opportunity to verify which users registered with their organization are still valid. While renewal does not require identity-proofing, all Entity/Agent Users and Investigative Search Users identities must be re-proofed every six years through the re-registration process.

No renewal process is established for Report Subjects as the account used to access the Report Response Service never expires. For Self-Query users, the NPDB-HIPDB account credentials expire at the time noted on their initial registration documents.

Trusted Operator accounts are valid until they are no longer employed; there are no specific renewal procedures for these accounts.

4.9.2 Account Update

Updating a NPDB-HIPDB account means changing the user profile information collected and stored in the system. Users may update their information through use of current NPDB-HIPDB credentials.

Trusted Operator accounts are updated by authorized System Administrators.

4.9.3 Account Revocation

The NPDB-HIPDB Entity/Agent Data Bank Administrator, Entity User, Authorized Agent, and Investigative Search User (i.e., Subscriber) accounts are revoked when the binding between the Subscriber and the NPDB-HIPDB account is no longer considered valid. Examples of circumstances that invalidate the binding are:

- The Subscriber violates, or NPDB-HIPDB suspects that the Subscriber is violating, the terms of this RPS, or any other agreement, regulation or law applicable to the account;

- The Subscriber is no longer affiliated with the registered entity, e.g., Subscriber's employment is terminated or Subscriber is suspended for cause, compromise, or suspected compromise of private keys and/or password and profile;
- The NPDB-HIPDB account has been, or is suspected of having been lost, or stolen;
- Change in Subscriber's role (such as organizational change where the Subscriber moves between Entities) or permissions;
- The Subscriber or other authorized party (as defined in Section 5.6) requests that the account be revoked.
- The Subscriber's Entity/Authorized Agent organization does not re-register with NPDB-HIPDB.

Self-Querier and Report Subjects may request their accounts to be revoked. The DPDB e-Authentication Manager or ISSO may also request revocation if the Subscriber violates or NPDB-HIPDB suspects that the Subscriber is violating the terms of this RPS, or any other agreement, regulation or law applicable to the account.

Trusted Operator accounts are revoked upon termination of employment or removal from the project.

5.0 Account Life-Cycle Operational Requirements

5.1 Registration

5.1.1 Who Can Submit a Registration Request

A document for registering an Entity shall be submitted by authorized representatives of the Entity/Authorized Agent, i.e. the Entity/Agent Certifying Official and Entity Data Bank Administrator, following the process described in Section 4.1.

Entity/Agent users shall be sponsored by their Data Bank Administrator(s) to register for an account following the process described in Section 4.3.

Investigative Search Users submit a notarized registration document directly to the NPDB-HIPDB to register for an account as described in Section 4.5.

Self-Query Users submit a notarized registration document and receive the self-query reports in the mail or access them electronically through the NPDB-HIPDB system.

Report Subjects receive initial account access information in the mail.

5.1.2 Enrollment Process and Responsibilities

As per the terms of the Subscriber Agreement that appears the first time a user logs into their account.

5.2 Registration Processing

It is the responsibility of the NPDB-HIPDB Document Control Center Operators to verify that the information in an Entity Registration document, Investigative Search User registration document and Self-Query is complete.

The Entity/Agent Data Bank Administrator shall follow the requirements specified in Section 4.3 to verify information in end user registration documents.

5.3 Account Issuance

The procedures for account issuance to NPDB-HIPDB subscribers are described in Sections 4.1– 4.7 of this document.

5.4 Account Renewal

The procedures for account renewal are described in Section 4.9.1 of this document.

5.5 Account Update

The procedures for account update are described in Section 4.9.2 of this document.

5.6 Account Revocation

5.6.1 Who Can Request Revocation

The revocation of an Entity/Authorized Agent Databank Administrator accounts may only be requested by:

- The Data Bank Administrator in whose name the account has been issued;
- The Certifying Official, if the Data Bank Administrator is an employee or contractor of the registered Entity or Authorized Agent;
- The DPDB e-Authentication Manager or ISSO.

The revocation of an Entity User, Authorized Agent or Investigative Search User account may only be requested by:

- The Subscriber in whose name the account has been issued;
- The individual or organization who made the request for the account on behalf of a device or application (for automated queries through IPT or QRXS);
- The Data Bank Administrator or Certifying Official, if the Subscriber is an employee or contractor of the registered Entity;
- The DPDB e-Authentication Manager or ISSO.

Self-Querier and Report Subjects may request their accounts to be revoked. The DPDB e-Authentication Manager or ISSO may also request the revocation of these accounts.

The ISSO makes a request to the Trusted Operator accounts upon termination of employment or removal from the project.

5.6.2 Requests for Revocation

The following information must be obtained for auditing purposes when a revocation request is made:

- Date of revocation request;
- Name of the Subscriber;
- Reason for requesting revocation;
- Name and title of person requesting revocation;
- Contact information of person requesting revocation;
- Signature of person requesting revocation (electronic signature if the Subscriber is requesting the revocation their own account via IQRS or a wet signature if the revocation form is submitted as a paper copy).

5.6.2.1 Revocation of the Entity Users, Authorized Agents and Investigative Search User Accounts

Entity Users, Authorized Agents and Investigative Search Users can make account revocation requests on-line using their existing NPDB-HIPDB credentials to their Entity/Authorized Agent Data Bank Administrators. Once the request is submitted, the Data Bank Administrator will review the request and revoke the account immediately upon verification of the request. In cases where the user cannot request revocation on-line through the NPDB-HIPDB system, the user will make the revocation request to the administrator through other channels (e.g., email, phone call); the Data Bank Administrator will send the NPDB-HIPDB account revocation form to the user. The user signs the revocation request document (no notarization required) and sends it back to the Data Bank Administrator. The Data Bank Administrator revokes the account and submits the document to NPDB-HIPDB for auditing purposes.

In cases requiring immediate revocation of an account, the requester may call the NPDB-HIPDB Customer Service Center and request the revocation. The Customer Service Center will send the NPDB-HIPDB account revocation form to the user. The user signs the revocation request document (no notarization required) and sends it back to the Customer Service Center. The Customer Service Center revokes the account and forwards the document to NPDB-HIPDB Document Center for auditing and archival purposes.

Faxed revocation request forms shall be accepted.

Entity/Authorized Agent Data Bank Administrators may revoke the user accounts based upon the revocation reasons stated in Section 3.9.3. The DPDB e-Authentication Manager and ISSO may also request the Customer Service Center to revoke user accounts based upon the revocation reasons stated in Section 3.9.3. In this case, the DPDB e-Authentication Manager or ISSO signs the revocation request document on behalf of the user and this document is archived for audit purposes.

5.6.2.2 Revocation of the Entity /Authorized Agent Administrator Accounts

The Entity/Authorized Agent Data Bank Administrator can make account revocation requests on-line using their existing NPDB-HIPDB credentials to the NPDB-HIPDB Customer Service Center. Once the request is submitted, the Center will review the request and revoke the account immediately upon verification of the request.

In cases where the Data Bank Administrator cannot access the account on-line or in cases requiring immediate revocation of an account, the Data Bank Administrator may call the NPDB-HIPDB Customer Service Center and request the revocation. The Customer Service Center will send the NPDB-HIPDB account revocation form to the Data Bank Administrator. The Data Bank Administrator signs the revocation request document (no notarization required) and sends it back to the Customer Service Center. The Customer Service Center revokes the account and forwards the document to the NPDB-HIPDB Document Control Center for auditing and archival purposes.

Faxed revocation request forms shall be accepted.

The Entity/Authorized Agent Certifying Official, the DPDB e-Authentication Manager or ISSO may also request the Customer Service Center to revoke the Data Bank Administrator accounts based upon the revocation reasons stated in Section 3.9.3. In this case, the Entity/Authorized Agent Certifying Official, the DPDB e-Authentication Manager or ISSO signs the revocation request document on behalf of the Data Bank Administrator and this document is archived for audit purposes.

5.6.2.3 Revocation of Self Querier and Report Subject Accounts

The Self Querier and Report Subject can make account revocation requests on-line using their existing NPDB-HIPDB credentials to the NPDB-HIPDB Customer Service Center. Once the request is submitted, the Center will review the request and revoke the account immediately upon verification of the request.

In cases where the Self Querier and Report Subject cannot access the account on-line or in cases requiring immediate revocation of an account, the Self Querier and Report Subject may call the NPDB-HIPDB Customer Service Center and request the revocation. The Customer Service Center will send the NPDB-HIPDB account revocation form to the Self Querier and Report Subject. The Self Querier and Report Subject signs the revocation request document (no notarization required) and sends it back to the Customer Service Center. The Customer Service Center revokes the account and forwards the document to NPDB-HIPDB Document Center for auditing and archival purposes.

Faxed revocation request forms shall be accepted.

The Entity/Authorized Agent Certifying Official, the DPDB e-Authentication Manager or ISSO may also request the Customer Service Center to revoke the accounts based upon the revocation reasons stated in Section 3.9.3. In this case, the Entity/Authorized Agent Certifying Official, the DPDB e-Authentication Manager or ISSO signs the revocation request document on behalf of the administrator and this document is archived for audit purposes.

5.6.2.4 Revocation of Trusted Operator Accounts

Trusted Operator accounts are revoked upon termination of employment or removal from the project. The ISSO makes the request to revoke these accounts.

5.6.3 Revocation Request Grace Period

There is no grace period for account revocation. Upon receipt and confirmation of the revocation request, the account is revoked. Once an account is revoked, the Subscriber must repeat the registration process to open a new account, including identity proofing.

6.0 Facility, Management and Operational Controls

6.1 Physical Controls

Specified in NPDB-HIPDB System Security Plan

6.1.1 Site Location & Construction

Specified in NPDB-HIPDB System Security Plan

6.1.2 Physical Access

Specified in NPDB-HIPDB System Security Plan

6.1.3 Power and Air Conditioning

Specified in NPDB-HIPDB System Security Plan.

6.1.4 Water Exposures

Specified in NPDB-HIPDB System Security Plan.

6.1.5 Fire Prevention & Protection

Specified in NPDB-HIPDB System Security Plan.

6.1.6 Media Storage

Specified in NPDB-HIPDB System Security Plan.

6.1.7 Waste Disposal

Specified in NPDB-HIPDB System Security Plan.

6.1.8 Off-Site backup

Specified in NPDB-HIPDB System Security Plan.

6.2 Procedural Controls

6.2.1 Trusted Operators

Specified in NPDB-HIPDB System Security Plan.

6.2.2 Number of Persons Required per Task

Specified in NPDB-HIPDB System Security Plan.

6.2.3 Identification and Authentication for Each Role

Specified in NPDB-HIPDB System Security Plan.

6.2.4 Roles Requiring Separation of Duties

Specified in NPDB-HIPDB System Security Plan.

6.3 Personnel Controls

6.3.1 Qualifications, Experience, and Security Clearance Requirements

Specified in NPDB-HIPDB System Security Plan.

6.3.2 Background Check Procedures

Specified in NPDB-HIPDB System Security Plan.

6.3.3 Training Requirements

Specified in NPDB-HIPDB System Security Plan.

6.3.4 Job Rotation Frequency and Sequence

No stipulation.

6.3.5 Sanctions for Unauthorized Actions

Specified in NPDB-HIPDB System Security Plan.

6.3.6 Contractor Requirements

Specified in NPDB-HIPDB System Security Plan.

6.3.7 Documentation Supplied to Personnel

Specified in NPDB-HIPDB System Security Plan.

6.4 Audit Logging Procedures

Specified in NPDB-HIPDB System Security Plan.

6.4.1 Types of Events Recorded

Specified in NPDB-HIPDB System Security Plan.

6.4.2 Frequency of Processing Data

Specified in NPDB-HIPDB System Security Plan.

6.4.3 Retention Period for Security Audit Data

Specified in NPDB-HIPDB System Security Plan.

6.4.4 Protection of Security Audit Log Data

Specified in NPDB-HIPDB System Security Plan.

6.4.5 Security Audit Log Data Backup Procedures

Specified in NPDB-HIPDB System Security Plan.

6.4.6 Security Audit Collection System (Internal vs. External)

Specified in NPDB-HIPDB System Security Plan.

6.4.7 Notification to Event-Causing Subject

Specified in NPDB-HIPDB System Security Plan.

6.4.8 Vulnerability Assessments

Specified in NPDB-HIPDB System Security Plan.

6.5 Records Archival

6.5.1 Types of Events Archived

Specified in NPDB-HIPDB System Security Plan.

6.5.2 Retention Period for Archive

Specified in NPDB-HIPDB System Security Plan.

6.5.3 Protection of Archive

Specified in NPDB-HIPDB System Security Plan.

6.5.4 Archive Backup Procedures

No stipulation.

6.5.5 Requirements for Time-Stamping of Records

Specified in NPDB-HIPDB System Security Plan.

6.5.6 Archive Collection System (Internal or External)

Specified in NPDB-HIPDB System Security Plan.

6.5.7 Procedures to Obtain and Verify Archive Information

Specified in NPDB-HIPDB System Security Plan.

6.6 Compromise and Disaster Recovery

6.6.1 Incident and Compromise Handling Procedures

Specified in NPDB-HIPDB System Security Plan.

6.6.2 Computing Resources, Software, and/or Data are corrupted

Specified in NPDB-HIPDB System Security Plan.

6.6.3 Token/Account Compromise Procedures

Specified in NPDB-HIPDB System Security Plan.

6.6.4 Business Continuity Capabilities After a Disaster

Specified in NPDB-HIPDB System Security Plan.

7.0 Technical Security Controls

7.1 Computer Security Controls

Specified in NPDB-HIPDB System Security Plan.

7.2 Life Cycle Technical Controls

7.2.1 System Development Controls

Specified in NPDB-HIPDB System Security Plan.

7.2.2 Security Management Controls

Specified in NPDB-HIPDB System Security Plan.

7.2.3 Life-Cycle Security Ratings

No stipulation.

7.3 Network Security Controls

Specified in NPDB-HIPDB System Security Plan.

7.4 Time-Stamping

Specified in NPDB-HIPDB System Security Plan.

8.0 Review of Registration Practices

8.1 Frequency of Review

NPDB-HIPDB Entities and Authorized Agents as well as all Customer Service Center/Document Control Center operators could be subject to an annual review of their registration practices. The NPDB-HIPDB CCB reserves the right to review or inspect registrations operations at any time. Further, the NPDB-HIPDB CCB reserves the right to inspect any information in the control or custody of any Data Bank Administrator pertaining to their identity proofing duties, or other obligations outlined within the Subscriber Agreement. This RPS will be reviewed annually and modified on an as-needed basis.

Current procedures for initial Entity/Agency registration and for new Entity User/Agent registration result in continuous auditing. For example: paperwork must be approved for all new Entity/Agency registrations before the account is created, and paperwork must be received and approved for all new Entity User/Agent accounts within 30 days or the account will be disabled.

Audit functions may be required for registered entities outside of the United States where notary services are not available, as they have self-certified. Audits may also be required to confirm account revocation procedures.

8.2 Identity/Qualifications of Reviewer

The reviewer must be familiar with the NPDB-HIPDB system, its operations, this RPS and any related documentation.

8.3 Reviewer's Relationship to NPDB-HIPDB

The reviewer (who meets the qualifications listed in Section 8.2 of this document) will be selected by the NPDB-HIPDB CCB to conduct the review.

8.4 Topics Covered by Review

This RPS, in its entirety, as well as all other supporting documentation is subject to annual review.

8.5 Actions Taken as a Result of Deficiency

The reviewer will report the results of a review to the CCB. The CCB will report the results to authorized authorities within HRSA and/or HHS, as appropriate. Any Entity or Authorized Agent being reviewed will propose a remedy, including the expected time for completion, to the CCB. Depending upon the nature and severity of the discrepancy, the CCB, in its sole discretion, may decide to halt temporarily the registration operation of the Entity, to revoke credentials issued to the Entity, or take other actions it deems appropriate. Upon correction of the deficiency, the CCB may reinstate the Entity. The CCB may require a special review to confirm the implementation and effectiveness of the remedy.

8.6 Communication of Results

The reviewer will report the results of the registration review to the CCB, HRSA and/or HHS, as appropriate. The implementation of remedies will be communicated to the CCB. A special review may be required to confirm the implementation and effectiveness of the remedy.

9.0 Other Business and Legal Matters

9.1 Fees

9.1.1 NPDB-HIPDB Credential Issuance or Renewal Fees

No stipulation.

9.1.2 Fees for other Services

No stipulation.

9.1.3 Refund Policy

No stipulation.

9.2 Financial Responsibility

No stipulation.

9.2.1 Insurance Coverage

No stipulation.

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance or Warranty Coverage for End-Entities

No stipulation.

9.3 Confidentiality of Business Information

All the NPDB-HIPDB information will be protected and only made available to authorized users or required by law.

9.3.1 Scope of Confidential Information

Personally Identifiable Information (i.e., PII) submitted in an NPDB-HIPDB registration document (see Table 1 *Identity Proofing an Entity User* for PII data collected) is considered sensitive. Access to the registration information (including user name and DBID number) will be restricted to Trusted Operations (Customer Service Center, Document Control Center, System Administrators) and others persons authorized by the CCB with a reason to know the information in order to perform their official duties.

9.3.2 Information Not Within the Scope of Sensitive Information

The information associated with the NPDB-HIPDB account, such as E-Mail address and Organization name are not considered sensitive.

For the purpose of proper administration of the accounts, this information may be requested to manage the accounts (e.g., identifying numbers, business addresses, telephone numbers).

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

Privacy Impact Assessment is conducted annually as required by HRSA. Refer to the NPDB-HIPDB privacy policy posted on the NPDB-HIPDB website for additional information.

9.4.2 Information Treated as Sensitive

All personally identifying information is considered sensitive and will be protected from unauthorized disclosure. Records of individual registration transactions may be released upon request to users involved in the transaction or their legally recognized agents. The contents of the archives maintained by NPDB-HIPDB shall not be released except as required by law.

9.4.3 Information not Deemed Sensitive

Some information that is provided during registration process such as E-Mail address, and Organization name are not considered sensitive.

9.4.4 Responsibility to Protect Sensitive Information

Sensitive information will be stored in the NPDB-HIPDB digital archive based on EMC Documentum and Paxton storage and may be released only in accordance with other stipulations in Section 8.4.

9.4.5 Notice and Consent to use Private Information

Per the NPDB-HIPDB privacy policy posted on the NPDB-HIPDB website.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

The NPDB-HIPDB shall not disclose private information to any third party unless authorized by the CCB, required by law, government rule or regulation, or order of a court of competent jurisdiction. Any request for release of information shall be processed according to 41 CFR 105-60.605.

9.4.6.1 Release to Law Enforcement Officials

In the event a user is suspected to have used, or is using, their credentials to commit illegal acts under the governing laws of the United States of America, upon presentation and verification of official court order or subpoena documentation and approval from HHS General Counsel, user credentials will be disclosed to law enforcement officials to assist in any investigative process. Any request for release of information will have its documentation authenticated. The authentication process requires that the receiver of the request:

- Verify the presenting official's credentials (at least one government-issued photo ID).
- Verify the subpoena or court order documentation presented by the official. This includes a sight check of the official letterhead and original signature, in addition to contacting the issuing office as specified on the document.
- Notifying the CCB prior to releasing the requested information.

9.4.6.2 Release As Part Of Civil Discovery

Registration information will be released in connection with civil discovery by subpoena, court order or otherwise as required by law. Unless prohibited by the terms of the order under which the civil discovery

is proceeding, the NPDB-HIPDB will make reasonable efforts to notify the end entity prior to releasing the information.

9.4.7 Other Information Release Circumstances

NPDB-HIPDB will not disclose any user credential information to any third party unless authorized by the NPDB-HIPDB CCB, required by federal law or regulation, or order of a court of competent jurisdiction.

9.5 Intellectual Property Rights

The U.S. Government retains exclusive rights to the intellectual property associated with any products or information developed under the NPDB-HIPDB RPS. Registrants and Subscribers represent and warrant that all information supplied during the registration process does not infringe upon or violate the intellectual property rights of any third party. Registrants and Subscribers will defend, indemnify, and absolve from financial responsibility NPDB-HIPDB for any claims of loss or damage resulting from such infringement or violation. If Registrants and Subscribers find it impossible to comply with this provision because Federal or State law prohibits indemnification or other compensation; NPDB-HIPDB will waive this provision because compliance would be contrary to law.

9.5.1 General

The intellectual property in this RPS is the exclusive property of HRSA.

9.6 Representations & Warranties

9.6.1 NPDB-HIPDB Representations and Warranties

NPDB-HIPDB warrants that any Trusted Agent relied upon by the system is operating in accordance with the applicable NPDB-HIPDB registration policies in place.

9.6.2 Subscriber Representations and Warranties

Subscribers are required to sign the Subscriber Agreement acknowledging their obligations.

9.6.3 Relying Parties Representations and Warranties

No stipulation.

9.6.4 Representations and Warranties of other Participants

None.

9.7 Disclaimers of Warranties

All responsibilities described in this RPS shall be adhered to – no disclaimers are permitted.

9.8 Limitations of Liability

The U.S. Government shall not be liable to any party, except as determined pursuant to the Federal Tort Claims Act (FTCA), 28 U.S.C. 2671-2680, or as determined through a valid express written contract between the Government and another party.

9.9 Indemnities

No stipulation.

9.10 Term & Termination

9.10.1 Term

This RPS becomes effective when approved by the CCB. This RPS has no specified term.

9.10.2 Termination

Termination of this RPS is at the discretion of the CCB.

9.10.3 Effect of Termination and Survival

The requirements of this RPS remain in effect through the end of the archive period for the last credential issued.

9.11 Individual Notices & Communications With Participants

This document does not restrict the channels (e.g., email, postal mail, telephone) used to communicate notices or changes in registration practices. No stipulation.

9.12 Amendments

9.12.1 Procedure for Amendment

The CCB shall review this RPS at least once every year. Corrections, updates, or suggested changes to this RPS shall be made available on a need-to-know basis to appropriate parties at HRSA and HHS.

9.12.2 Notification Mechanism and Period

This RPS and any subsequent changes shall be made available to appropriate parties within one week of approval.

9.13 Dispute Resolution Provisions

In the event of any dispute or disagreement between two or more of the participants (Disputing Parties) arising out of or relating to these policies, including Relying Party and Subscriber Agreements, the Disputing Parties shall use their best efforts to settle the dispute or disagreement through negotiations in good faith following notice from one Disputing Party to the other(s). If the Disputing Parties cannot reach a mutually agreeable resolution of the dispute or disagreement within sixty (60) days following the date of such notice, then the Disputing Parties may present the dispute to the NPDB-HIPDB CCB. In the event that the NPDB-HIPDB CCB is unable to resolve the dispute, the parties may bring the matter to the HHS Office of General Counsel for resolution.

9.14 Governing Law

The construction, validity, performance, and effect of certificates issued under these procedures shall be governed by United States Federal law (statute, case law, or regulation).

9.15 Compliance with Applicable Law

NPDB-HIPDB is required to comply with applicable laws.

9.16 Miscellaneous Provisions

9.16.1 Entire agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

If a particular provision of this RPS is determined to be invalid, illegal, or unenforceable, the remaining provisions of this RPS shall remain in full force and effect until the RPS is updated.

9.16.4 Enforcement (Attorneys' Fees and Waiver of Rights)

No stipulation.

9.16.5 Force Majeure

No stipulation.

9.17 Other Provisions

No stipulation.

10.0 Document Change History

The table below identifies all changes that have been incorporated into each baseline of this document. Baseline changes require review and approval.

Version	Date	Author	Description
1.0k	6/11/10	Savith Kandala, Kathy Rigney	First draft for DPDB review.

Appendix A: Acronyms

Listed below are acronyms used within this document.

CCB	Change Control Board
DBID	Data Bank Identification Number
DCN	Document Control Number
DPDB	Division of Practitioner Data Banks
FTCA	Federal Tort Claims Act
HIPDB	Healthcare Integrity and Protection Data Bank
ID	Identification
IQRS	Integrated Query and Reporting Service Query and Reporting XML Service
ISC	Investigative Search Capability
ISSO	Information System Security Officer
ITP	ICD Transfer Program
NIST	National Institute of Standards
NPDB	National Practitioner Data Bank
OMB	Office of Management and Budget
ORI	Originating Agency Identifier
PII	Personally Identifiable Information
QRXS	Query and Reporting XML Service
RPS	Registration Practices Statement
TIN	Tax ID Number