

## My Continuous Query Story: Coreen



“We were absolutely new to Continuous Query,” remembers Coreen, an authorized agent with 16 years of experience querying and reporting to the Data Bank. Her hospital group began using the service in January 2012 as part of an organization-wide efficiency sweep: “It was something that was definitely put on the hospital group’s ‘to-do’ list,” Coreen adds. Before the initiative, each of the 11 hospitals and 4 outpatient surgery centers in her health system were responsible for their own credentialing, and each did their own One-Time Querying and reporting. Now, the Credentialing Verification Office (or CVO, for which Coreen is the Authorized Agent) oversees the centralized credentialing of all 4,000 practitioners throughout the

health system, all of whom are enrolled in Continuous Query. As a result, the hospitals and surgery centers now receive automatic notifications whenever there is a new report available on any of their enrolled practitioners. The Board of Directors for each entity makes the hiring, credentialing, and privileging decisions.

The time savings achieved through Continuous Query has drastically improved how the CVO operates. “The best thing about all of this has been the amount of time we save. We no longer have to stop and query the Data Bank on all these practitioners. We know [the querying’s] already done, because the practitioners are enrolled in Continuous Query. Whether it was a new applicant, or someone we were reappointing every two years, or a request for a new privilege, it was very time-consuming to make that a part of the process. In any given month, we’d have about 100 practitioners due for querying.”

**“The best thing about all of this has definitely been the amount of time we save. We no longer have to stop and query the Data Bank on all these practitioners.”**

In addition to Continuous Query, use of the subject (or practitioner) database has increased her efficiency by removing hours of manual data entry from her busy schedule. To store the practitioners in the subject database, Coreen, with initial help from her organization’s Information Technology department and the Data Bank’s Customer Service Center, imported her organization’s in-house practitioner database into her Data Bank account’s subject database and then into the Continuous Query service using the XML format. The subject database pre-populates querying and reporting forms with a practitioner’s data, greatly simplifying these Data Bank tasks. In addition,

**“It’s like night and day.”**

Coreen finds it “a very easy process” to regularly upload updates from her health system’s database into the Continuous Query database.

Not only has Continuous Query saved her time, but it has delivered more useful and timely information. “It’s like night and day,” notes Coreen, adding, “now, the practitioners are in the

subject database and in Continuous Query, and if there is something [added], you know you're going to get a report, and if not, you keep going forward."

## Protecting PII: Your Responsibilities as a Data Bank User



As a Data Bank user, you are required to protect the confidentiality of all Personally Identifiable Information (PII) to which you have access. This includes the handling of your Data Bank Identification Number (DBID), user ID, user password, and the personal practitioner information you use when submitting a query or report. The confidential receipt, storage, and disclosure of information is essential to the Data Bank, and accountability at all levels is important. The yearly Rules of Behavior agreement, acknowledged by every user prior to accessing the Data Bank system, also points out the importance of protecting this information.

PII includes information that can be used to identify a unique individual, either alone or when combined with other information. Examples of PII include, but are not limited to:

- Name: full name, maiden name, mother's maiden name, or alias.
- Personal identification numbers: Social Security Number, passport number, driver's license number, taxpayer identification number, financial account number, or credit card number.
- Address information: street address or email address.
- Telephone numbers: mobile, business, or personal.
- Personal characteristics: photographic images, x-rays, fingerprints, or other biometric images (retina scans, voice signatures, etc.).

### Tips for Safeguarding PII

- Sensitive information must never be left unattended, even temporarily. When visitors are present, place sensitive documents out of sight and close any revealing computer screens.
- Remove sensitive information from desks, printers, copy machines, and computer screens after business hours. At the end of the day, store sensitive information in a secure area.
- Dispose of sensitive information properly: paper documents should be cross-cut shredded before disposal.
- PII should not be stored on a laptop unless there is a specific need, written management approval is granted, and the data is password protected and encrypted.
- Transmit sensitive information securely: information transmitted via email should be password protected and encrypted as an email attachment.

- PII should not be stored on removable or personal digital media (CDs, flash drives, tapes, diskettes, hard drives, etc.).
- Never fax sensitive information.
- Transport sensitive information securely: Data or sensitive information delivered via U.S. Postal Service or courier should be placed in a safety-sealed envelope and labeled "Confidential Information to be Opened by Addressee Only."

## What is Self-Query?

**What?** The Data Bank offers the self-query service to allow practitioners and organizations to query on themselves to see if there are reports that have been submitted on them in the Data Bank.

**Why?** Practitioners can self-query either for their own interest; or at the request of a potential employer, licensor, or insurance provider.

**When?** Practitioners and organizations can query on themselves as often as they like. There is a \$16 fee for each self-query, which includes one hard copy in the mail and access to the report online for 45 days.

**How?** Practitioners and organizations start the self-query process on the Data Bank [website \(http://www.npdb-hipdb.hrsa.gov\)](http://www.npdb-hipdb.hrsa.gov).

If your organization interacts with practitioners or requests that they submit a self-query, we hope that you will pass this information along to them so they can take advantage of this easy-to-use process!



## Dear Data Bank



This column responds to questions about Data Bank policies and procedures. If you have a question, please email "[Dear Data Bank](mailto:help@npdb-hipdb.hrsa.gov)." We look forward to hearing from you!

### **Do I need to report administrative fines to The Data Bank? What about continuing education requirements?**

Administrative fines, civil monetary penalties, and continuing education requirements are not reportable unless they are considered a negative action, are the result of a formal proceeding, and are 1) connected to the delivery of health care services or 2) taken in conjunction with an adverse licensure or certification action. If one of these two conditions is met, an administrative fine, civil money penalty, or continuing education requirement would be reportable to the Data Bank under Section 1921 of the Social Security Act.

If you have a specific question with which you would like assistance, please contact the Data Bank via [email \(help@npdb-hipdb.hrsa.gov\)](mailto:help@npdb-hipdb.hrsa.gov).