

Instructions for Completing the Request for NIMRS Access (RFA) Form

The Request for NIMRS Access (RFA) form is used to request access for individual staff members **OR** to change the security group of staff with existing access. These instructions describe the process for filling out and submitting the RFA form. The NIMRS Unit can be reached at 518-474-3619 if you have additional questions.

Instructions for completing & submitting the RFA:

RFA Form

1. Enter the staff member's (the new NIMRS user) contact information.
2. Select a Security Group (see below for additional detail regarding Security Group options)
3. The form must be signed by both the "Requestor" (staff member) and the "Local Facility NIMRS Administrator" (a security manager, quality director or supervisor). Both signatures must be original – faxes or photocopies cannot be processed.
4. Page 2 of the RFA should be used to request access to multiple providers when an affiliation exists and staff are shared.

Memo

Write a memo using your facility's letterhead and list the names of staff requesting access. If you intend to transfer an existing token from one employee to another, list both names in the memo and include the serial number of the token. The serial number is on the back of the token. If you have a token for an employee you no longer authorize to use NIMRS, and you do not wish to reassign this token, please explain this in the memo and return the token in the request package.

Mailing Instructions

Mail the completed RFA and the required memo to the address below. **Originals only – no faxes or photocopies.**

**NYS Office of Mental Health
6th Floor BQI – NIMRS Unit
44 Holland Ave.
Albany, NY 12229**

Security Groups

The NIMRS system has several security groups, each with its own set of access rights in the system. Some of the more commonly used groups are described below:

- Risk Management: highest level access with the ability to enter incidents, report externally to OMH and Commission on Quality of Care for the Mentally Disabled (CQC), run trend reports, and perform maintenance activities. **We recommend that at least two staff be assigned Risk Management access so if one becomes unavailable, the other will be able to report incidents.**
- Clinical Supervisor: mid-level access with ability to enter most data on incident reports (can't complete the QCC-100 for patient deaths). This group cannot report incidents externally to OMH or CQC.
- Clinical Line Staff: lowest level access with ability to enter limited data on new incidents. This group does not have access to the search function so users cannot view or edit previously entered incidents.
- **The higher level groups incorporate the rights of the lower ones so it is sufficient to select only one group.**

This is the REQUEST FOR NIMRS ACCESS Form

REQUEST FOR NIMRS ACCESS

(FOR NON-OMH EMPLOYEES)

STATEMENT OF CONFIDENTIALITY - Information contained in any Office of Mental Health (OMH) database is confidential and legally protected under Federal and New York State law and applicable OMH policy or standards. The information may be accessed only with specific authorization by OMH. Misuse of any data or application system, including inappropriate access to or use of information from the database will subject the individual to administrative, civil and criminal disciplinary action. Print-outs, photo copy or facsimile of confidential information may only be made by authorized users and must be secured and properly disposed of in accordance with Mental Hygiene Law, OMH policy and OMH Security Standard and Procedure Manual. No information will be released to any source other than those authorized. All computer resources are restricted solely for the conduct of business with OMH consistent with the terms and conditions as set out in the signed agreements (CDA, CAGA and/or DCA). Personal and unauthorized usage is prohibited.

1. Type the information for each user (one user per form).

2. This field is left blank unless the user already has an OMH issued User ID.

3. User signs and dates here.

4. Supervisor or Administrator signs and dates here.

5. For Security Group, select only one group per user. Your facility will need at least 2 Risk Management users. (If you have questions, call 518-474-3619, and we will help you select your groups.)

6. Enter name and date for for each signature.

TO BE COMPLETED BY OMH:

BQI OMH Groupwise Email Account for this user: Yes No Initials: _____ Date: _____

Security Unit - Token Serial No. _____ Initials: _____ Date: _____

LAN - Groupwise Email Account (User is external - NIMRS Local)

Groupwise Userid _____ Initials: _____ Date: _____

**Do Not Write On Your Form
Below This Line
It is for OMH Use Only**

**Do Not Write On Your Form
Below This Line
It is for OMH Use Only**

REQUEST FOR NIMRSWEB ACCESS - PAGE 2
(FOR NON-OMH EMPLOYEES)

Additional Agency Information

--	--

Agency Name: _____

Business Address: _____

City, State, Zip: _____

Telephone No.: _____ ext: _____

Agency Name: _____

Business Address: _____

City, State, Zip: _____

Telephone No.: _____ ext: _____

Agency Name: _____

Business Address: _____

City, State, Zip: _____

Telephone No.: _____ ext: _____

Agency Name: _____

Business Address: _____

City, State, Zip: _____

Telephone No.: _____ ext: _____

Agency Name: _____

Business Address: _____

City, State, Zip: _____

Telephone No.: - - ext: _____