LEVELS OF ACCESS AND MASKING in MHS Mart (M2)

The system will support the eight classes of users described below, based on the level of access appropriate to each user.

The Commander, Director, or other Head of each entity that is authorized slots is responsible and accountable for designating the appropriate class of access for those users designated for that entity. EI/DS must maintain two lists to support this function. One list identifies the point-of-contact to whom each entity leader has delegated authority to perform this function. The second list is the list of authorized users and their assigned levels of access as designated by the point-of-contact.

Designation of access authority by the Commander does not in any way diminish the responsibility of EI/DS to verify the appropriate documentation is on hand for any user permitted access to Privacy Act data. To safeguard the data from possible access after a user has left a position, DoD Regulations require freezing accounts after 120 days of non-use and terminating accounts after 365 days of non-use. Consequently, the account will be frozen for any M2 user that does not sign-on and execute a query within a 120 day period. After 365 days of non-use, the account will be terminated.

For those users authorized full access to non-privacy act granular data (classes III and IV), Privacy Act fields must be hidden. At this time, only patient names and sponsor Social Security Numbers (SSNs) are viewed as Privacy Act data that must be hidden. In order for this class of users to follow unique (if anonymous) individuals, the sponsor SSN must be scrambled and available in an alternative visible field and the Sponsor Rank (Pay Grade) must be collapsed into seven categories (see Appendix A for algorithm). The M2 FPG supports a calculated scrambled identifier over one embedded in the data to permit periodic rotation of the scrambling algorithm, provided that: (1) users are notified well ahead of time when the algorithm is to change and 2) the method does not degrade the functionality of the system. HPA&E will provide the scrambling algorithm, which will be the same for all data types.

Classes of Users

|  |  |  |
| --- | --- | --- |
| Granularity of Data | Privacy Act Data | Non-Sensitive Data |
| Summary |  | I: Report ViewerII: Expert User |
| MTF-specific | V: Local Management | III: Local Policy |
| Unlimited | VI: Super User | IV: High Level Policy/MgtIVa: PublisherIVb: High Level Policy/Mgt for Level V user |

Each access category could be operationalized as:

* Level I: Report Viewer. The default user would be a report viewer, who gets access to summary tables only, and is not able to launch queries against the database itself. This implies that the user can view and drill down in canned reports, but cannot alter or build reports. WEB-I was intended to be the primary method to satisfy this level of access.
* Level II: Expert User. These users are more empowered than the default user in that their access to summary tables is not constrained by the canned reports, and they have the ability to alter or create new reports from the summary data cubes. They do not have access to the granular database.
* Level III: Local Policy User. Such a user addresses and analyzes trends, data, and data quality, but has no need to know patient identities. Originally, it was hoped this kind of user could be served with WEB-I using the “drill through” functionality. However, it was discovered that “drill through” could not be provided without opening the door to complete freedom to write and edit reports, making this class of user as resource-intensive as the higher classes. One choice is to limit the class to “masked fields” (see section to follow), and to place them in MTF groups unable to select rows that do not contain the user’s MTF DMIS ID family in any of the DMIS ID fields
* Level IV: High Level Policy User. Such a user is similar to the local user but cannot be restricted to a local domain. (Examples include users from major commands, SGs, and HA/TMA.) Implementation options are the same as for Local Policy Users, but without the row selection limitation. A variant to this definition applies to the Coast Guard – Level IV for the Coast Guard will limit users to Coast Guard beneficiaries and facilities (limits users to those persons whose “sponsor service” is Coast Guard; or for care delivered at a Coast Guard treatment facility; or for a person who is enrolled to a Coast Guard treatment facility; see Appendix B for actual implementation rules).
* Level IVa: High Level Policy User (Publisher). This access level is designated for existing users who have been granted authorization to publish reports to Corporate Documents. These users will be approved by the cognizant M2 FPG representative. Publishing users may also have a user ID at a higher level of access for their own use of M2. If so, the additional ID as a publisher will not count against the FPG representative’s M2 account quota. This is the highest level of access permitted to publish to corporate documents.
* Level IVb: High Level Policy User (Second Account for Level V User). This access level is designated for existing users who have already been granted Level V access. All Level V users are not automatically granted an additional account—the Level IV account must be requested. If the additional ID is granted, it will not count against the FPG representative’s M2 account quota.

* Level V: Local Management User. Such a user must know patient identities for some questions. (Examples of positions that might need such access include managed care functions, clinician functions, claims / benefit functions, and enrollment functions.) These users would not be limited to “masked fields”, but would be in MTF groups unable to select rows that do not contain the user’s MTF DMIS ID family.
* Level VI: Super User. Such a user has defined or ad hoc responsibilities too broad to restrict access to the data. (Examples include the central data processors, authorized builders of reports for broadcast within a command, and probably at least one identified super user of each organization. Because of the Super User’s very broad access to sensitive data, it is essential that their knowledge of Privacy Act rules and restrictions is rigorous.) This is the unrestricted access level currently enjoyed by most full client users. A variant to this definition applies to the Coast Guard – Level VI for the Coast Guard will limit users to Coast Guard beneficiaries and facilities (limits users to those persons whose “sponsor service” is Coast Guard; or for care delivered at a Coast Guard treatment facility; or for a person who is enrolled to a Coast Guard treatment facility; see Appendix B for actual implementation rules).

Appendix A: Sponsor Rank (Pay Grade) Collapsing Algorithm

| **Object Class** | **Rank Group Algorithm** |
| --- | --- |
| **EJ** | **ES** | **OJ** | **OS** | **WO** | **CD** | **XX** |
| * Institutional Detail
* Non-Institutional Detail
 | 00-04 | 05-09 | 20-23 | 24-31 | 11-15 | 19 | All Others |
| * DEERS Person Detail
* TRICARE Enr Detail
 | Pay Plan ’ME’ and Pay Grade 00-04, 10 | Pay Plan ’ME’ and Pay Grade 05-09 | Pay Plan ’MO’ and Pay Grade 00-03 | Pay Plan ’MO’ and Pay Grade 04-11 | Pay Plan ’MW’ and Pay Grade 00-05 | Pay Plan ‘MC’ | All Others |
| * Direct Care Admissions Detail
* Direct Care Outpatient Encounters Detail
 | E1-E4 | E5-E9 | O1-O3 | O4-O9, 10, 11 | W1-W5 | Sponsor Pay Grade=CD or Patient Category Code=A14, C14, F14, N14 | All Others |

\* EJ = Enlisted, Junior; ES = Enlisted, Senior; OJ = Officer, Junior; OS = Officer, Senior; WO = Warrant Officer; CD=Cadet; XX = Other (students, civil servants, unknowns (e.g., those without distinction as to whether officer or enlisted)).

**Appendix B: Coast Guard Access Implementation Rules**

**A variant of Level IV and VI for the Coast Guard (CG) will limit users to CG beneficiaries and facilities - that actual implementation limits those users in all tables to those persons whose "sponsor service" is CG. However, they are also allowed to see any other direct care encounter record for care delivered at a CG treatment facility (CGTF), or for a person who is enrolled to a CGTF, which is actually implemented as described in the remaining bullets.**

* **The treatment facility filter is only needed for direct care encounters (SADRs) and prescription fills (PDTS). No CGTF provides inpatient care, so direct care admissions (SIDRs) are like all the other data types.**
* **For all data types, a record should be viewable if the sponsor service is Coast Guard, or if the treatment or enrollment military service is Coast Guard. In practice, this means we place all Coast Guard DMIS IDs in one overall parent DMIS ID family, representing the Coast Guard. That way enrollment to or treatment in any Coast Guard DMIS ID will be visible to this group.**
* **A Coast Guard user who should only see his own clinic can have normal Level 5 (or 3) that would only let them view records of care delivered at that CGTF DMIS ID. Since there are no PRISMs or catchment areas with CGTF DMIS IDs, this is a normal Level 5 as it exists today, using the single child DMIS ID in the user group authorized**.