

MDS/OASIS Systems Security

The following information is intended to be a guide for nursing home administrators and staff responsible for backing up and protecting Minimum Data Set (MDS) and Outcome and Assessment Information Set (OASIS) data.

Introduction - Centers for Medicare and Medicaid Services (CMS) has requested that the states remind administrators of their responsibility to assure that their local MDS data is backed up. This is part of assuring that medical records are safe. A number of unexpected problems can occur with electronic data, both MDS and other records: A hard drive may fail or a computer may be stolen. Files can be mistakenly overwritten or deleted. A natural disaster such as fire, flood, or earthquake may damage software/hardware. CMS expects administrators to make sure that staff regularly back up data.

DATA PROTECTION:

The protection of all resident data regardless of the format (hardcopy or electronic) is the responsibility of the health care facility under the Privacy Act (5 U.S.C. 552a). The Privacy Act specifically addresses these issues such as the penalties for destruction and/or disclosure of individual identifiable information. Data protection includes confidentiality, system security and storage.

DATA CONFIDENTIALITY:

Confidentiality is controlling personal and confidential information and controlling the release of information to others. Health care facilities should develop procedures and responsibilities for data confidentiality in all areas including contractors (e.g. software vendors, consultants and transmission services), mailing lists, electronic transmission, and telephone conversations. Penalties are prescribed in the Privacy Act (5 U.S.C. 552a) for failing to protect the confidentiality of resident data.

DATA SECURITY:

Health care facilities are responsible for the protection of data, from accidental or malicious destruction, disclosure, or modification. If circumstances threaten the security of your database, contact the MDS/OASIS Help Desk immediately at (916) 324-2362.

DATA RECOVERY PLAN:

A disaster recovery plan is essential in reclaiming important data lost in a disaster. A disaster recovery plan generally includes:

- **Alternative storage/facility** – A place where backup data is stored and operations can continue.
- **Equipment Priorities** – A list of equipment to be replaced in order of its importance.
- **Personnel Needs** – A list of personnel and their respective responsibilities.
- **Program and Output Reconstruction** – The plan should include the procedure for the recovery of programs and data. Prioritize the software to be loaded and schedule to be operational.
- **Back-up** – A disaster recovery plan also includes the day-to-day back-up procedures and data storage. Consider the use of a tape back up.
- **Power back-up** – For protection against power interruption through the use of an alternate power supply (also known as an uninterruptible power supply) and at a minimum a reliable surge protector.

A good disaster recovery plan should be in writing and all persons affected by it should have a copy and understand it. For disaster recovery to be fast and complete, procedures must be defined, responsibilities clearly understood, and it must be practiced.