

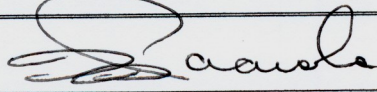
# ARIZONA-1 DMAT

## STANDARD OPERATING PROCEDURE

**Subject:** Employee Medical Records Security Policy

**SOP NO.**  
03-11

**Approved by  
Team Commander:**



**Effective Date:**  
8/31/11

### A. STATEMENT OF PURPOSE

The purpose of this policy is to comply with the laws and regulations on responsibility practices regarding the maintenance of medical records including Health Insurance Portability and Accountability Act of 1996 (HIPPA) enacted by the U.S. Congress and defined as Protected Health

Information requirements are identified in the Privacy Rule and Security Rule. This policy shall apply to any and all records or data with any patient identification information.

### B. POLICY

The medical records that are kept by AZ-1 pertain to Pre-deployment Medical Screening and follow-up to determine fitness for deployment as employee's of the National Disaster Medical System (NDMS). The records include: physical fitness (walk/run; stair climb, and tote carry); an affidavit of fitness; a signed self answered medical history with vital signs and BMI; and medical letter and statement for follow-up of NDMS disqualifiers. In some instances, there may be a report of illness or injury on deployment that will be filed in the medical records. Claims for injury or illness as the result of deployment will be kept by the Administrative Officer.

It is the responsibility of the Medical Branch Director to protect and safeguard the information and information systems against unauthorized user(s). This policy statement applies to the security and confidentiality of employee information created electronically or paper documents.

### C. PROCEDURE

#### **Definitions:**

##### **Confidentiality:**

The act of limiting the disclosure of private matters. It refers to an expectation that information shared by an individual with a provider or Medical Branch Director during the course of reporting or care will be used only for its intended purpose. The use of health information without the patient's knowledge and consent is a violation of confidentiality.

##### **Security of Protected Health Information:**

To control access to or modification of protected health information.

##### **Security Standards:**

Security standards are established to ensure that patient-identifiable information remains confidential and protected from unauthorized disclosure, alteration or destruction. The HIPPA mandated the adoption of security standards for all healthcare facilities. Security includes the physical and electronic protection of the integrity, availability, and confidentiality of computer based information and the resources used to enter patient information. The security of the records includes the storing, processing, and communication of all patient identifiable data.

**C. PROCEDURE CONT.**

Security will be maintained by the following means:

1. Medical records will remain in the possession of the Medical Branch Director.
2. Medical records will be secured in one locked area when not in use.
3. Medical records may be brought to team meetings for the purpose of collection and adding to the records, review by the individual team employee, and signature of the Team Commander.
4. Individual team employees may review their own information at any time.
5. Prior to deployment and after being notified of rostering or deployment,
  - a team employee will complete an electronic copy of the Pre-deployment Medical Screen form from the team website and directly mail it to the Medical Branch Director, emailing the form will imply consent to add the employee's electronic signature.
  - **OR** a team employee will complete a paper copy of the Pre-Deployment Medical Screen form from the team website, sign the form, scan it, and e-mail the completed, signed form to the Medical Branch Director. The Medical Branch Director will review the Pre-deployment Medical Screen form and previous Pre-deployment Medical Screening forms for disqualifiers and, then mark and sign the form (actual or electronically). The Pre-deployment Medical Screening form will then be sent to the Team Commander for review and signature prior to deploying the team employee. The Administrative Officer will then be notified of the team employee's fitness for deployment.
6. With electronic transfer of the medical record, security must be maintained by ensuring correct email addresses.
7. A hard copy of electronic medical records forms will be maintained in the Medical Branch Director medical files.
8. Electronic medical records will not be stored on a computer hard drive. They may be stored on a CD or flash drive and maintained in the Medical Branch Director medical files.
9. When mailing medical records to the NDMS Chief Medical Officer for waiver requests, all records will be sent with a Return Receipt Requested to ensure that they arrived at the correct destination. Waiver responses will be sent back in a like manner.

**Removal or Destruction of Records:**

If the employee has a claim for injury or illness as a result of deployment, the medical record will be maintained indefinitely.

Otherwise, a medical record will remain in the files as long as the person is an employee of AZ-1 DMAT or a related NDMS team.

- When an employee resigns from the team, that individual's medical records will be destroyed by shredding.
- If an employee transfers to another NDMS team, the individual team employee must request the medical record in writing.
- The individual then assumes full responsibility for his medical record upon transfer.