

Acceptable Use Policy For Tripler Army Medical Center's Sensitive Information Systems

As a Tripler Army Medical Center (TAMC) computer user, your actions can greatly increase or decrease the integrity, availability, and confidentiality of information. Protecting that information is called "Information Assurance" and you are an integral part of that protection program. These are the minimum guidelines for use and do not exempt users from further restrictions that may be imposed by this Command.

Threats, vulnerabilities, and risks. Since almost all of TAMC's computers are networked, your computer has access through the Local Area Network (LAN) to the NIPRNET. The NIPRNET is our connection to the Internet. This internetworking of computers makes your computer a gateway to vast amounts of sensitive information. Basically, a risk accepted by one imposes a risk on all. Since your computer is "trusted" by other computers within the military domain, it provides access to various military networks. "Trusted" means that other computers recognize your computer as a Department of the Army (DA) computer. As such, you can obtain passwords and gain access to certain information not available to non-Army users. Based on that, your actions can put your computer, TAMC's network, and all Army computer networks at risk.

Information security objectives. The Privacy Act of 1974 and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) impose responsibilities on all personnel to prevent misuse or compromise of personal data to include patient data. There are three main considerations.

Confidentiality of Information. Most of the information processed on TAMC systems is sensitive personal and/or medical information. Only certain personnel are authorized to disclose this information. Access to this information in a system does not authorize any user to disclose such information to persons not having a need to know it. Browsing of patient information for anything other than official duties is prohibited.

Data Integrity. Patient treatment decisions are made from the information in a system. All information entered into a system must be accurate and remain that way.

Data Security. The Privacy Act requires safeguards for confidential records. All users are responsible for preventing accidental or malicious alteration, destruction, or disclosure of personal information.

Procedures for creating, changing, and safeguarding passwords. TAMC systems will prompt you to change your password every 90 days. Passwords need to consist of the following four items - upper case, lower case, number, and special character. With our current audit trail capability, we have individual accountability. Basically, your password is you. Do not share your password with anyone else. And always log off any system when leaving it unattended so that someone else does not use your password. To log off a PC, hit CTRL+ALT+DEL, select "Log Off," and click "OK." If you forget your password, you will need to show a photo ID before the password is reset.

Procedures for monitoring log in attempts and reporting discrepancies. TAMC systems are the property of the Army and the Army is fundamentally the Internet service provider for official duties and obligations. As such, it is subject to monitoring for enforcement of ethical or acceptable use, management, Operations Security, unauthorized access, log in attempts, verification of security procedures, etc. You should have no expectation of privacy on data you process, store, or transmit while using Government equipment. Your use of any TAMC system, authorized or unauthorized, constitutes your consent to monitoring.

Unauthorized activities. Certain activities are never authorized on Army networks. These activities include, but are not limited to, any personal use of Government resources involving pornography or obscene material (adult or child); copyright infringement (such as sharing copyrighted material by means of peer-to-peer software); gambling; the transmission of chain letters; unofficial advertising, soliciting, or selling except on authorized bulletin boards established for such use; of any activity in violation of any statute or regulation.

Authorized systems configuration and associated configuration management requirements. Tripler now has an Enterprise Management System (EMS). With this system, your PC is configured and controlled from a central location. This speeds up receiving upgrades to software and troubleshooting any problems you may have. Anti virus software updates are pushed to each PC in the same way. In order to receive all these upgrades, it is critical that PCs not be turned off at any time so these

security patches can be pushed to them as needed. Approximately once a month, you should completely restart your PC to insure maximum efficiency. Modems are not authorized for use within TAMC. Screen saver features automatically lock the PC after five minutes of inactivity requiring reauthentication before unlocking the system. Privately owned hardware and software is prohibited on TAMC workstations.

System data and access controls. Only authorized personnel will be allowed access to any system. Supervisors determine who needs what type of access to which systems. Data must be protected in a system as well as it would be in hard copy printouts. Storage media as well as paper products should not be left unattended unless secured in a locked area. Data storage media that is no longer usable will be turned in to the Information Assurance Manager (IAM) for destruction. Paper products may be destroyed by using a cross-cut shredder that cuts 1/2" x 1/32" or by using the Confidential Paper and Shredding Recycling System which has sealed bins located throughout the hospital where sensitive paper products may be placed until picked up and destroyed.

Physical and environmental considerations necessary to protect the system. During non-duty hours or when an area is left unattended, doors will be locked to prevent theft or manipulation of hardware, software, or data. Telephones will be placed a minimum of 39 inches from any part of an information system to prevent electronic emanations of sensitive data. Situate your monitor to prevent inadvertent viewing from windows, doorways, or personnel passing near the computer. There are no special environmental considerations when systems are being used within TAMC.

Incident, intrusion, malicious logic, virus, abnormal program or system response reporting requirements. Suspected or actual security incidents will be reported to the IAM at 433-5033 immediately upon discovery. Incidents include, but are not limited to, any indication of an unauthorized user attempting to access a system; using access privileges to gain information protected under the Privacy Act for other than official use; or allowing, either intentionally or negligently, another person to use a personal password.

Information Operations Condition (INFOCON) requirements and definitions. INFOCONS are based on a combination of threats, vulnerabilities, incidents, and real-world conditions. The INFOCON system presents a structured, coordinated approach to react and defend against adversarial attacks on TAMC computers, networks and telecommunications. The four steps are INFOCON ALPHA (increased risk of attack) - this condition is declared when an increased risk of attack on information systems exists. INFOCON BRAVO (specific risk of attack) -this condition is declared when there is evidence of a specific risk of attack on the information infrastructure. INFOCON CHARLIE (limited attack) - this condition applies when an actual information attack occurs or when intelligence indicates the possibility of an imminent information attack that could result in significant operational impact. INFOCON DELTA (general attack) - this condition applies when general attacks against information systems networks seriously degrade readiness and operations. When an INFOCON is declared, you will be notified of the specific protective actions you need to take.

Emergency and disaster plans. All systems have recovery/restoration plans in place. However, you will need to backup your personal mission-essential files through the use of diskettes, local back up tape drives, or by copying the files to a network server.

Sanctions. Penalties may include loss of use or limitations on use of equipment or services or prosecution under the Uniform Code of Military Justice or the United States Code (5 U.S.C. 552a(1)).

I have read the above information regarding the use of TAMC automated systems. I understand my responsibilities regarding these systems and the information contained in them.

(Printed Name)

(Signature)

(Date)