POLICY:	**EMAIL, INTERNET, AND OTHER SOCIAL MEDIA SERVICE USAGE – 100.02**		
APPROVAL:	**VICE PRESIDENT OF PROFESSIONAL SERVICES; MANAGER OF EMS;**		
EFFECTIVE DATE: 7/15/2024			**ORIGINAL EFFECTIVE DATE: 08/16**
DEPARTMENT SPECIFIC		**EMERGENCY MANAGEMENT SYSTEM**	

I. Purpose:

The purpose of this policy is to set forth standards related to EMS provider's use of email, internet and other social media services while working under the direction of the Morris Hospital Emergency Medical Services (EMS) System.

II. Definitions:

A. EMS Providers:

A primary or secondary status provider functioning as an Emergency Medical Dispatcher (EMD), Emergency Medical Responder (EMR), Emergency Medical Technician (EMT), Paramedic, Pre-Hospital Registered Nurse (PHRN), Emergency Communications Registered Nurse (ECRN).

B. Users:

Individuals who have been granted authorization to access to the electronic pre-hospital record, or other Morris Hospital & Healthcare Centers (MHHC)network connections.

C. Email:

MHHC's system for sending and receiving messages electronically over its computer network.

D. Network:

A group of many interlinked local area networks and leased lines in the wide area network typically under the management of the same organization. The private communications network that is contained within an organization is called an Intranet. The main purpose of an intranet is to share system information and computing resources among EMS providers.

E. Social Media:

A number of web based communication vehicles that enables users to interact with and learn from each other's, and to share information electronically through an organizations intranet and internet systems. Social Media includes, without limitation, podcasting, video-casting, blogs, discussion forums, Wiki sites and other online and network related resources, such as:

1. Blog: a web log or website chronicling the reflection's or interest of the writer.

2. Social Media Websites: On-line communications of people linked by their shared interests (e.g., TikTok, WhatsApp, SnapChat, YouTube, Facebook, Twitter, Pinterest, Instagram, LinkedIn, etc.)

3. Wiki: Technology that enables people to create, edit or link to web content. Wikipedia, a free, user-written encyclopedia, is a well-known Wiki site.

4. Podcast, Video Cast: A digital file distributed over a network, such as the Intranet/Internet. (e.g., Buzzsprout, Megaphone, Podbean, Libsyn, Blubrry, etc)

5. Discussion Forums: Websites and email sites that permits Users to post questions, responses, and other comments (e.g., Reddit, bulletin boards, chat rooms).

6. Miscellaneous and New: Miscellaneous and new communication and connection services over networks to enable communications (e.g., RSS feeds hyperlinks).

F. Network Services:
For the purpose of this policy, includes the definitions of *network* and *social media* as stated.

G. Protected Health Information (PHI):
Any health information that can be used to identify a patient and information related to health care operations, health care services provided to a patient, or the payment for services provided to a patient. PHR includes:

1. All medical records and other information which identifies that patient, including demographic, medical and financial information
2. Information in any form whether electronic, paper or spoken.

III. Procedure:

All users of MHHC email and network services must use these services in an appropriate manner and protect the information on them. Users of MHHCinformation have the responsibility to protect that information in a manner consistent with the best interests of the Morris Hospital EMS System/MHHC.

A. Acceptable Use Statements:

1.1. Subject to Monitoring: MHHC reserves the right to access, monitor, or disclose, as it deems necessary the contents and history of each users email messages and network services activity for any purpose. MHHC may also disclose a user’s activity and its content to law enforcement officials and/or MHHC management, System without the user’s consent or prior notice to the user.

2.1 Shared Accounts: Shared email and network accounts are not allowed. IDs and passwords are unique to individual users and must not be shared with other users.

2.2 Secure Confidential Information over un-trusted Networks: Information that contains confidential information of PHI that is transmitted using the Internet or other public networks must be secured. Email that stays within Morris Hospital network is secured and protected; however Internet email is not secured by default and requires that user to encrypt data prior to transmission. Emails both internal and external should only include the minimum information required to get the point across. If there is a requirement to send an encrypted message outside MHHC network, use Secure: in the subject line of an email.

B. Prohibited Use: The use of email and network services for a function that could harm the MHHC/Morris Hospital EMS System infrastructure, expose proprietary or confidential information, or create legal liabilities, or that is not appropriate to fulfill EMS duties is prohibited. The following are examples of prohibited use:

1. Fraud and Unethical Use:

a. Misrepresenting oneself, or inappropriately representing the Morris Hospital EMS System

b. Any misrepresentations/fraud to gain unauthorized access to a computing system or network

c. Unauthorized decrypting or attempted decrypting of any system or user passwords or any other user's encrypted files.

d. Using the email account of another individual without express permission or proxy.

e. Solicitations that are not specifically approved by Morris Hospital EMS system policy.

f. Posting or mentioning identifiable MHHC or Morris Hospital EMS system patient health information (i.e., PHI) through network services (i.e., any social media such as Facebook).

g. Posting or mentioning of sensitive MHHC or Morris Hospital EMS System business information though Network Services

h. Use of hacking software, hacking passwords, and attempting to disable or bypass security controls.

i. Sending messages which include content, copies, or file attachments of documents or computer software in violation of copyright laws.

j. Engage in any unauthorized activities for personal financial gain. Place advertisements for commercial enterprises, including but not limited to, goods, services or property

k.

2. Service Impacting:

a. Any unauthorized or deliberate action that damages or disrupts computing systems or networks.

b. Willfully introducing a computer virus, Trojan horse or other destructive program into the MHHC network systems or into external systems or network.

c. Use of non MHHC Information Technology USB devices including, but not limited to USB flash drives, cameras, mobile phones, webcams, keyboards, and mice is not permitted.

3. Offensive/Discriminating Behavior:

a. Communications that are demeaning, defaming, harassing (including sexually), or discriminatory against any person.

b. Access, display, storage, or distribution of offensive, discriminatory, or pornographic material that is otherwise inconsistent with or in violation of the mission or values of the Morris Hospital EMS System or contributes to an intimidating or hostile environment for all individuals, patients and providers.

4. Disclosure of Confidential Information:

a. Accessing and/or disclosing PHI or other confidential information that is not within the scope of ones role as an EMS system provider.

b. Dissemination of proprietary, strategic, confidential, private or otherwise restricted information without appropriate approval is prohibited.

5. Social Media and Online Activities:

a. Providers must never post or mention identifiable MHHC or Morris Hospital EMS System patient information (i.e., PHI), or proprietary or confidential information of MHHC. This includes, but is not limited to photos, discussion or other such postings related to an individual patient's care, our colleagues, business operations or other activities regarding Morris Hospital EMS System patients.

b. Providers must not check personal email or instant messaging accounts while using a MHHC or Morris Hospital EMS System computer.

In addition to the policy, guidelines and practices set forth as above, a Morris Hospital EMS System provider's responsibility as a healthcare professional must follow standards that are stricter than standards for the general Social Media user community. Specifically and to the extent applicable, EMS System providers are expected to be familiar with, commit to and follow this policy as written.

IV. Implementation / Sanction / Validity

A. The EMS Medical Director or Manager of EMS may suspend from participation within the System any prehospital provider that does not adhere to the Morris Hospital EMS System standards.

1. MHHC; computing systems are shared resources. Therefore, any action that inhibits or has the potential to inhibit the ability of others to utilize these resources will be considered a policy violation. Because MHHC cannot enumerate all possible violations

that might arise, MHHC will evaluate situations not expressly addressed in this policy on a case-by-case basis. prehospital provider of Morris Hospital EMS System are expected to exercise good judgment in their use of MHHC systems. Users should contact the IT department, the EMS Medical Director or Manager of EMS when questions arise regarding potentially inappropriate computer usage or if they suspect unauthorized activity of their accounts. If MHHC detects that an account has been accessed in violation of MHHC's policies or that specific account activity may pose a risk to the system as a whole, that account may be disabled without warning.

2. Users of MHHC computing resources are responsible for the actions performed on their accounts. If an individual has any knowledge of unauthorized use of his or her account, he or she is in violation of this policy and is responsible for any actions taken by the unauthorized user. In addition, any activity that takes place under a user's ID will be considered to have been done by the owner of that account.
3. Any prehospital provider who discovers a violation of this Policy shall notify the EMS Medical Director or Manager of EMS.
4. This Policy does not supersede the provisions of MHHC IT, privacy, or security policies, procedures, or guidelines in force at departmental or other levels or any applicable law or regulation. All applicable policies, procedures, laws, and regulations must always be observed.

Approval:

James Kirchner **VP of Professional Services**	**Date**	**Kathleen Geiger, MSN, RN, RN** **Manager of EMS and Emergency Management**	**Date**