POLICY:	**EMAIL, INTERNET, AND OTHER SOCIAL MEDIA SERVICE USAGE – 300.28**		
APPROVAL:	**VICE PRESIDENT OF PROFESSIONAL SERVICES; MANAGER OF EMS;**		
EFFECTIVE DATE: 9/1/2016	**CURRENT REVIEW/REVISION DATE: 8/16**	**SUPERSEDES: N/A**	**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 network connections.

C. Email:

Morris Hospital'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., 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.

5. Discussion Forums: Websites and email sites that permits Users to post questions, responses, and other comments (e.g., 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 Morris Hospital email and network services must use these services in an appropriate manner and protect the information on them. Users of Morris Hospital information have the responsibility to protect that information in a manner consistent with the best interests of the Morris Hospital EMS System/Morris Hospital.

A. Acceptable Use Statements:

1.1. Subject to Monitoring: Morris Hospital 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. Morris Hospital may also disclose a user's activity and its content to law enforcement officials and/or Morris Hospital 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 Hospita network is secured and protected; however Internet email is not secured by default and requires that user to encrypt data prior to transmission.

B. Prohibited Use: The use of email and network services for a function that could harm the 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 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 Morris Hospital EMS System business information though Network Services

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 Morris Hospital network systems or into external systems or network.

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:
   Providers must never post or mention identifiable Morris Hospital EMS System patient information (i.e., PHI), or proprietary or confidential information of Morris Hospital. 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.

   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.

Approval:

Thomas J. Dohm	**Date**	**Robin Stortz, RN**	**Date**
VP of Professional Services		**Manager of EMS**	