

Hurley Medical Center
Standard Practice

Information Network and Electronic Communication User Policy

Policy:

1. This document serves as the acceptable use policy for use of Hurley Medical Center's network and its network connection to the Internet.
2. This document applies to both Hurley provided and privately owned devices that access or utilize Hurley's network as well as to all Internet*, Electronic Communication**, and Social Media*** activity conducted by on duty personnel.
3. Hurley Medical Center is committed to providing an environment that encourages the use of computers, electronic information and computer networks as essential tools to support the mission of patient care, teaching and research. The information systems in use at Hurley Medical Center and the information within the systems fall within the policies, guidelines and employee work rules for patient confidentiality, HIPPA guidelines, and Hurley's confidential information.

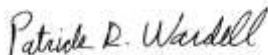
Procedures:

1. Use of Hurley Medical Center's network and internet connection:
 - a. Employee network or Internet access is to be used for Hurley-related purposes only.
 - b. All employee Internet activity is subject to this policy and managerial approval at all times while the employee is on duty.
 - c. Internet activity not directly related to job function is forbidden at all times in any patient care areas or other highly visible locations.
 - d. Visitor or patient Internet access is available through the HurleyGuestNet wireless network only.
 - e. All of Hurley's network usage, including Internet access, is monitored, recorded, and reviewed. There is no reasonable expectation of privacy. Hurley Medical Center reserves and intends to exercise the right to review, audit, intercept, access and disclose all traffic sent over Hurley's network or Internet connections for any purpose. The information acquired and properly obtained for legitimate business or legal purposes may be disclosed to appropriate parties without the permission of the employee.
 - f. Hurley retains the right to filter internet or network traffic as it sees fit. Attempting to circumvent any filter put in place is forbidden.
 - g. Hurley retains the right to block individual device access to the network or internet as it sees fit without warning. Attempting to circumvent any blocks put in place is forbidden.
 - h. All electronic data, including personal data and photos, stored in any Hurley systems are the property of Hurley Medical Center and can be deleted or removed without warning if deemed inappropriate.
 - i. Accessing or sending pornographic, obscene, or illegal material is forbidden.
 - j. All files downloaded from the Internet or any other source must be checked for computer viruses. Up to date virus protection is mandatory and any attempts to disable anti-virus software is forbidden.
 - k. Downloading or installing third party or outside software without the prior approval of IT is forbidden with the exception of document readers and software loaded for the purpose of being a part of an online conference or webinar.
 - l. Remember that items posted to the Internet contain Hurley's electronic trail that can be tracked directly back to the individual computer and user that posted it. Care should be taken when posting anything.
 - m. Do not post any items on the Internet that do not reflect the policies or values of Hurley.
 - n. Hurley has provided remote desktop software for system support and maintenance. Any unauthorized access to Hurley systems using any third party proxy access software such as GoToMyPC or other methods is forbidden.
 - o. Attempting to disable or block remote desktop or other administrative software or restrictions on a Hurley owned device is forbidden.
 - p. Use of Hurley's Internet connection to operate a business, or for financial gain is forbidden.
 - q. Non-Hurley owned network devices such as routers, wireless access points, or switches are forbidden from the Hurley network unless approved in advance by the I.T. department.
 - r. Use of Hurley's Network for hacking or any hacking related activities is forbidden.
 - s. Use of file sharing or peer-to-peer applications is forbidden.

Supersedes Bulletin Dated: 2/12/97

Distribution: All Departments

Originating Department: Information Technology



Hurley Medical Center
Standard Practice

Information Network and Electronic Communication User Policy

2. Use of Electronic Communications and Social Media:

- a. While the employee is on duty all electronic communications and social media access are to be used for Hurley-related purposes only.
 - b. Electronic communications are not considered private despite any such designation either by the sender or the recipient.
 - c. The existence of passwords, "message delete" functions, and encryption, do not restrict or eliminate Hurley Medical Center's ability or right to access electronic communications. Hurley Medical Center reserves and intends to exercise the right to review, audit, intercept, access and disclose all messages created, received or sent over the Hurley system for any purpose. The contents of communications properly obtained for legitimate business or legal purposes may be disclosed to appropriate parties without the permission of the employee.
 - d. Sending confidential information**** through any electronic communication system or social media is forbidden. Exceptions may be granted with the approval of the department Vice President and the Chief Information Officer and communications must be sent using Hurley Medical Center's encryption software.
 - e. Sending or purposely receiving pornographic, obscene, illegal, or significantly business inappropriate material is forbidden through any hurleymc.com e-mail address at any time or through any electronic communication or social media mediums while the employee is on-duty.
3. Any employee who violates this policy or uses the Internet or Hurley network for improper purposes shall be subject to discipline, up to and including, termination of employment.

Definitions:

* Internet Activity

Access to any site or service outside of Hurley's private network through any mechanism including but not limited to wired or wireless access through Hurley's primary internet connection, using a publicly available 802.11 connection such as HurleyGuestNet, or through a privately owned mobile data link such as a 3G / 4G cellular connection.

** Electronic Communications

Communication utilizing a computer or mobile device by means of text, images, audio, video, or other data, but not including a traditional phone-to-phone voice conversation. Examples include but are not limited to e-mail, Skype, SMS or MMS (cellular phone text / picture messaging), or web postings.

*** Social Media

Forms of electronic communication through which users create online communities to share information, ideas, personal messages, and other content. Examples include but are not limited to Facebook, Twitter, LinkedIn, Foursquare, and YouTube.

**** Confidential Information

Any non-public information including but not limited to protected health information(PHI), social security numbers, financial information, contracts, personnel information, business strategies, and AutoCAD or engineering diagrams.

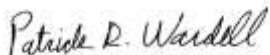
Responsibility:

1. Senior administrative staff and department heads are responsible for insuring that all managers, supervisors, and employees are periodically briefed on this policy.
2. All management and supervisory staff are responsible for ensuring compliance with this policy.
3. All employees are responsible to ensure personal compliance with this policy.

Supersedes Bulletin Dated: 2/12/97

Distribution: All Departments

Originating Department: Information Technology



Patrick R. Wardell, President and CEO