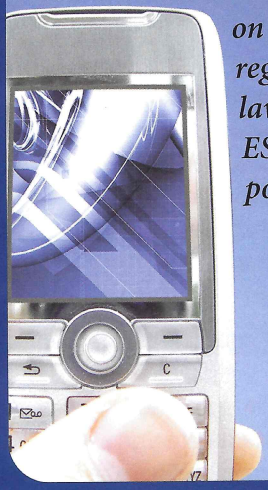
Employment Practices Update

Bringing important information to emergency service organizations

VOLUME 08 • NUMBER 2

ESO leaders have a heightened responsibility to educate their members on privacy regulations, laws and ESO policies.



Also Available –
Cellular Telephone Use in EMS Communiqué
Visit http://www.vfis.com/resources.htm

VFIS®
A Division of Glatfelter Insurance Group

Published by the
Glatfelter Insurance Group
York, Pennsylvania

Risks You Face in a Wireless World:
Camera Phones, Emails, and Internet

Let's call them unintended consequences—images or information from camera phones, PDAs (personal digital assistants), Internet and emails that pose risks to your Emergency Services Organization (ESO). Living in a wireless world, ESO members can use technological devices anywhere, anytime, for any purpose, and not necessarily in the best interests of the ESO. Confidentiality of incident information is a requirement for all responders. Even word of mouth discussions regarding the details of an incident can be harmful to the ESO. Consider the following scenario of a violation of patient privacy.

> *While responding to a private residence or business, a member of your ESO takes unauthorized pictures from his camera phone and later posts the photos on an EMS industry web site. The ESO member's intention was to share information for educational purposes with other EMS professionals. However, a patient in the photographs could be identified, and the patient's treatment records are plainly visible in another photograph. Moreover, local media could discover the disclosure of such sensitive and confidential information.*

The scenario described above puts the ESO at risk on several levels. The ESO and/or its members could be susceptible to civil liability or criminal prosecution. Personal privacy violations or other confidentiality breaches could equate to HIPAA (Health Insurance Portability and Privacy Act) violations. ESO members could be disciplined up to and including termination for violating ESO policy. Such misuse of technology will certainly result in harm to the ESO's reputation and diminished public trust.

This article explores how your ESO can take reasonable measures to protect its employees and volunteers, as well as community members, from privacy violations stemming from abuses of technology, particularly cell and camera phone usage. There is clearly tangible value in the appropriate usage of scene photographs for injury documentation, communication with the receiving facility to assist in treatment, ESO training purposes and quality assurance. Nevertheless, safeguards must be in place to ensure proper utilization of such technologies.

Duty to Prevent Privacy Violations

In emergency services, breaching patient confidentiality and possible HIPAA violations are primary concerns with taking on-scene photo or video images and audio recordings, or even discussing the incident with anyone. The *Standards for Privacy of Individually Identifiable Health Information*, often referred to as the HIPAA Privacy Rule, was established to protect certain health information. The U.S. Department of Health and Human Services issued the Privacy Rule to address the use and disclosure of individuals' health information, called "protected health information." The Privacy Rule protects all individually identifiable health information held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper or oral.

A major goal of the Privacy Rule is to ensure that individuals' health information and medical

Continued on page 2

Continued from page 1

records are properly protected while allowing the flow of health information needed to provide and promote high-quality health care and to protect the public's health and well-being. The Privacy Rule strikes a balance that permits important uses of information, while protecting the privacy of people who seek care and healing.

The Office of Civil Rights is responsible for enforcement of HIPAA privacy regulations. Civil and criminal penalties can be imposed against covered entities (i.e., emergency medical providers) that violate the privacy rights of their patients. Overall, an ESO must be diligent to protect all documentation regarding patient care.

ESO Responsibilities

ESO leaders must hold their employees and volunteers (members) to high standards of ethics and behavior, while conducting official ESO business, on ESO-property or during an ESO-related event. This starts by developing standards for responders on confidentiality of information from incidents at the most basic level, by word of mouth. In today's technological environment, this includes developing standards and regulations for members using camera or cell phones and other electronic communications. Your ESO must take reasonable measures to:

- Prevent abuses of technology.
- Set up multiple reporting avenues or procedures to discover such member abuses—questions, concerns or policy violations should be directed to the immediate supervisor, supervisor's supervisor, human resources manager or lead administrator/chief officer.
- Promptly investigate and take any necessary action against members known or suspected of technology abuses.
- Prevent future occurrences of misuse or abuse.

Cell/Camera Phone Usage Policies

Some experts estimate that as many as 80 percent of Americans own a cell phone. With cell phones now equipped with digital cameras, camcorders and audio recorders, the potential for abuse is multifaceted. ESOs are left scrambling to develop policies and procedures that are current with ever-changing technology. Your ESO is encouraged to consult with local legal counsel to construct a comprehensive electronic communications systems policy, that encompasses cell and camera phone usage.

There are many issues to consider when developing and implementing a policy regarding cell or camera phone usage.

Should the ESO ban or simply limit cell phone usage? Some ESOs prohibit possessing or using personal cell phones altogether while on duty. This policy stance is not likely realistic considering the need for ESO members to easily communicate with family members (e.g., a sick child) when on "down time." However, an ESO may limit how, where and, most important, when a member may utilize a personal cell phone. For instance, ESO rules may state that personal cell phones must be kept on "silent" or "vibrate" modes while on duty. The ESO policy may state personal cell phones may not be utilized from the time an emergency call is dispatched until it is cleared.

Remember that hand-held cellular or PDA devices also allow text messaging, sending or receiving email, and surfing the Internet. The goal is for cell phones to not distract from or otherwise interfere with the member's ability to perform the essential functions of the job.

How should the ESO policy address the camera, video and audio functions on cellular devices? It is understandable that, while on the job, ESO members would occasionally need to use the telephone function of their personally owned cellular device, but problems for the ESO typically arise when members utilize the camera, video or audio functions. In fact, it is difficult to come up with many scenarios when a member must, for business-related purposes, use the camera, email, Internet or audio recording functions of a personally owned cellular device or PDA. Consequently, many ESOs strictly prohibit using the camera, video and audio functions of a member's personal cell phone while on the job. This policy stance can help limit the possibility of unauthorized photos on an emergency scene or other sensitive images captured in the station, such as in sleeping quarters and bathrooms.

How should the ESO define permissible camera usage? Your ESO should be careful to assign who within the organization has the authority to take on-scene photos, while clearly defining the limited usage of the resulting images. ESO policies and procedures should communicate clearly that any photos, videos or other images taken within the scope of employment or membership duties are the sole property of the ESO.

Under no circumstances should an ESO member distribute any photographs, videos or other images to any individual or entity outside the organization, such as the media, speaking engagements, or a website, including the ESO's site, an emergency services industry site or personal sites (such as MySpace or YouTube). The ESO should designate a Privacy Officer or Administrator to help the organization comply with HIPAA or other confidentiality regulations or laws. Permission to take photographs, videos or audio recordings should only be granted to designated members as provided by the ESO in writing.

Training and Education

Technologies are quickly evolving and becoming easier to access and utilize. Particularly given the sensitive personal and medical information that is available in the emergency services environment, ESO leaders have a heightened responsibility to educate their members on privacy regulations, laws and ESO policies. ESOs should present valuable education and training in a live setting, whenever possible, to allow for interaction and question/answer periods. Signed member acknowledgments are also important to help ensure a consistent message is communicated and understood through policy, procedure and training. Proper precautionary measures can help keep private information about citizens and your ESO from falling into the wrong hands.

Michael McCall, J.D., provides employment practices consulting and training to emergency service organizations nationwide.