The Hawthorn CONNECTION

EST. 1978 Q3 August 2016 10820 Sunset office Dr., 3rd Floor, St. Louis MO 63127 800-899-5757

H.E.R.O.E.S. Care: *(Homefront Enabling Relationships, Opportunities, and Empowerment through Support)*

H.E.R.O.E.S Care provides support to all branches of the military families in the communities where they live. They provide emergency financial aid, employment opportunities and mental health care services through a network of specially trained care givers before, during and after deployment. They also provide quality care packages to deployed soldiers.

The program consists of a network of tens of thousands of trained caregivers and thousands of professional mental health care and service providers working together to provide an unprecedented system of support for military members and their families.

Military members must provide for all of their own personal care items while deployed and many military families do not have the financial resources to send these items to their deployed family member. The cost of a quality care package can exceed $100.00. Care packages from groups and organizations not only provide an important "taste of home," but allow these families to preserve precious financial resources.

Hawthorn's ERC (Employee Recognition Committee), commanded by Laura Woodham, Human Resources Coordinator, held a drive this year and delivered over 5 boxes of supplies to them.

Laura Woodham: "Thank you to everyone who supported this worthy cause, great job."

Cybercrime & Ransomware Update: by Stan Hosler

Cybercrime is once more in the news as ransomware attacks in 2016 have targeted hospitals. Ransomware criminals lock computers in place and charge a fee to unlock the system.

In February of 2016 the Hollywood Presbyterian Medical Center in Los Angeles was attacked by ransomware, and the hospital later admitted they paid the $17,000 ransom in bitcoins. It has been reported that the success of this attack has led to the subsequent targeting of other hospitals.

In March of 2016 the Methodist Hospital in Henderson, Kentucky was forced to shut down its desktop computers and transfer operations to its backup system. The system was apparently hacked through phishing emails that contained the Locky malware. Patient files were locked and the hackers demanded a ransom to unlock the system. Officials at the hospital worked through the emergency and declined to pay the ransom.

A local TV station reported that the Kansas Heart Hospital in Wichita was attacked by ransomware in May of 2016. According to this report the hospital admitted to paying an unspecified amount of ransom, but the criminals failed to decrypt the hostage files. The hospital then declined to pay a second ransom for the same attack.

Additional hospitals targeted in 2016 include the Chino Valley Medical Center in Chino, California and Desert Valley Hospital of Victorville, California. Not all attacks are reported, and it is possible that some hospitals have paid ransoms to avoid negative publicity.

The urgency of patient care makes hospitals more vulnerable to ransomware than other businesses and institutions. Health care providers need instant access to patient records, and lives are literally on the line while the hospital is held hostage. Additionally, security measures at hospitals lag behind other institutions, such as banks and other businesses. Hospitals have been very focused on HIPAA compliance and patient privacy, but many hospitals have not trained their employees on security awareness.

Most experts are recommending that hospitals improve their security protocols. One of the simplest procedures is to arrange for backup files and frequently scheduled backups. In the case of Methodist Hospital, cited above, it was the hospital's backup systems that enabled rapid restoration of data and resolution of the problem.

In July 2016 the Centers for Medicare & Medicaid Services (CMS) issued guidance on ransomware. The new guidance indicates that ransomware attacks should be reported as a breach of HIPAA security, even if the hospital believes no data was lost and no files were locked.

RACTrac is a Tool for Advocacy:

by Stan Hosler

Since 2010 the Centers for Medicare & Medicaid Services (CMS) have used recovery audit contractors (RACs) to audit payment claims to hospitals. The American Hospital Association (AHA) conducts quarterly surveys among participating hospitals to collect information program can be improved. The AHA uses the RACTrac data to help members navigate the appeals process and to advocate for RAC policy changes.

RACTrac results for the most recent survey, first-quarter 2016, indicated that surveyed hospitals are appealing 47% of all RAC claim denials, and 60% of reviewed claims did not have an overpayment. Further, more than 80% of claims appealed to an administrative law judge took longer than 90 days required by law. Visit the AHA website (www.aha.org) to learn more about RACTrac surveys and RAC advocacy.

2016 Q3 Employee Service Awards

Lisa B. **15 year Anniversary**

Laura B. **10 year Anniversary**

HAWTHORN
PHYSICIAN SERVICES CORPORATION

Addressing Complexity with Certainty