EIN PRESSWIRE

Enhanced EHR Security through TPM in Healthcare Computers

As a response to a heightened need for Electronic Health Record Security, Teguar now offers Trusted Platform Module (TPM) on medical grade computers.

CHARLOTTE, NC, USA, May 29, 2015 /EINPresswire.com/ -- According to a ProPublica internet article post in February of 2015, there have been more than 78 million people who were affected by health data breaches. A pilot study conducted in 2011 and 2012 showed that 102 of 115 organizations reviewed had some problems with data security. The security of electronic health records has now become a national point of concern. The types of information contained in these records are ever expanding, leaving the consumer more vulnerable. Identity information, financial information as well as genetic information is now stored in electronic medical records. There are many ways to manage these threats. One basic way is through secure healthcare computers.

On HealthIT.gov, the US government has released safety recommendations which include over nine main areas for keeping electronic healthcare records safe. One of the main areas listed is the system interface. The recommendation for healthcare computer hardware in relation to system interfaces is as follows:

“At the time of any major system change or upgrade that affects an interface, the organization implements procedures to evaluate whether users on both sides of the interface correctly understand and use information that moves over the interface. Security procedures, including role-based access, are established for managing and monitoring key designated aspects of interfaces and data exchange.” (HealthIT.gov, “Policymaking, Regulation, & Strategy: Health IT and Safety”)

In order to hit these SAFER recommendations put out by the Office of the National Coordinator (ONC) it is important to actively manage what data moves across healthcare computers. One way to secure the transferring of data is through a Trusted Platform Module. The Trusted Platform Module (TPM) gets installed on the motherboard of a computer and works to secure health record information through a number of ways. Data encryption, network access control, authentication and a secure boot are features that safeguard valuable EHRs.

As a response to this increasing need for EHR safety, Teguar Computers has released a new product feature on some of their Medical Grade Computers. The new TM-3040-19R All-in-one medical computer has TMP 1.2 included as a feature for those who want to step up their EHR security. This feature is intended to compliment the other hardware medical specific features that are already included in Teguar medical computer offerings. The TM -3040-19R has over fifteen input output ports so that users can control the configuration of their hardware setup. A Core i3/i5/i7 processor with up to 8GB ram is also included to quickly facilitate the flow of information.

Patient record security will continue to be a hot button issue as the medical industry continues to move towards 100% integrated EHRs. The medical computer hardware industry currently has solutions to help. Upgrading to a new hardware platform such as the TP-3040-19R with TPM will help optimize your medical technology goals. Teguar Corporation is proud to be offering this cutting edge technology. Contact sales@teguar.com for further information.

Company Profile:
Headquartered in Charlotte, NC, Teguar is a leading manufacturer of fully enclosed fanless and medical grade All-In-One computer solutions. Teguar medical computers are designed to perform 24/7 in extreme healthcare environments. We also ensure that our staff is up to date with the most innovative technology and always offer state-of-the art solutions to meet the fast changing market demands. With Teguar’s hardware, customers can build a reliable system and experience a fast Return of Investment.

Press release courtesy of Online PR Media: http://bit.ly/1G8Fs08

Shira Sagal
Teguar Computers
(704) 960-1761
email us here

This press release can be viewed online at: http://www.einpresswire.com

Disclaimer: If you have any questions regarding information in this press release please contact the company listed in the press release. Please do not contact EIN Presswire. We will be unable to assist you with your inquiry. EIN Presswire disclaims any content contained in these releases.