

Network Steps Up PHI Protection

The importance of protecting Seton's patient health and financial information cannot be overemphasized. While the Ponemon Institute's Benchmark Study on Patient Privacy and Data Security found that data breaches cost health care organizations an average of \$1 million annually and the health care field as a whole \$6 billion per year, the damage to Seton's reputation when breaking trust with patients is incalculable.

The passage of the Health Information Technology for Economic and Clinical Health Act in 2009 widened the scope of privacy and security protections under HIPAA to provide stronger safeguards for patient data. Any individual or entity that wrongly obtains or discloses PHI may face criminal penalties and civil fines up to \$1.5 million.

The Department of Health and Human Services declared encryption of electronic data and destruction of paper data as the only two methods capable of rendering PHI unusable, unreadable or indecipherable. As such, the Seton Healthcare Family is stepping up its encryption technology to further protect patients' and workforce members' sensitive medical and confidential information, such as social security or credit card numbers.

On April 25, 2011, Seton's new Data Loss Prevention tool began scanning all outbound e-mail and attachments for unsecured transmissions that could put the network and its patients at risk of HIPAA violations or identity theft.

Going forward, any e-mail containing protected health information or other confidential information must include the text [SECURE] or [PHI] in the subject line when sent to any non-seton.org address. This includes messages sent to Ascension Health addresses and many Seton-associated facilities such as physician offices, City Community Health Centers and the Travis County Health Care District. Your recipient will receive an e-mail with a hyperlink to a secure portal where your message awaits.

Please note that failure to add [SECURE] or [PHI] into the subject header of appropriate e-mail correspondence (as shown above) stops the message from going out.

If you think an e-mail you attempted to send has been stopped in error, please send a message explaining the situation to dlp@seton.org. Your feedback will be reviewed by the privacy officer and the Information Services Security team monitoring the Data Loss Prevention tool. Please understand that an exception rule cannot be created to allow data that meets this criterion, but is not actual financial or protected health information (such as test data used to validate a Seton application), to pass through the Data Loss Prevention tool.

