Central Texas ACHE
Leading Information Safety:
Planning for Data Privacy and Security

On Tuesday, April 28th, the Central Texas ACHE chapter hosted an event, "Leading Information Safety: Planning for Data Privacy and Security". While enjoying a breakfast bounty prepared by St. David's Medical Center staff, Aaron Franklin, Mimir Health addressed current problems, ethical concerns and potential solutions regarding healthcare data security, followed by a panel discussion with Thomas Thrower, Austin Diagnostic Clinic CIO, John Southrey, Manager, Consulting Services, Texas Medical Liability Trust and moderated by Charles Durant, FACHE.

According to the Identity Theft Resource Center, forty-three percent of reported breaches in 2014 occurred in the healthcare space. Since information found within an individual's health record can net between five hundred and one thousand dollars, this growing trend poses significant concern for healthcare providers. And while only one-fifth of healthcare organizations have reported a breach, the potential for multiple additional violations exist due to small (<500 persons) or undetected infractions not being identified. Fees for a HIPAA security violation can reach $1.5M; however, there are additional costs for notifying individuals, providing credit monitoring fees, public relations campaigns and legal fees.

What can your organization do to prevent breaches? While most healthcare organizations set aside three percent, allocating five to six percent of your total IT budget for breach prevention represents a step in the right direction. In addition, ensure that your organization is, at minimum, compliant with HIPAA and Texas HB300 (HB 300 takes HIPAA a few steps further, and here are a few highlights of what it adds):

- Organizations must train their employees on federal and state laws within 90 days of on-boarding, with biannual retraining thereafter
- Extends the definition of a Covered Entity to essentially anyone who touches PHI for commercial or professional gain
- Further restricts the use of PHI for sales and marketing activities
- Adds Texas Attorney General penalties separate from US HHS violation penalties

In addition, work with organizations (Business Associates) who demonstrate commitment to data security best practices and provide leadership in your role that promotes data security. Identify and implement low hanging fruit such as data encryption, secure messaging, strong passwords and single sign-on systems. Finally due to the self-reporting requirements and corporate social responsibility borne by healthcare providers, breaches should be reported in order to aid the HHS and OCR develop policy for current realities.

With special appreciation for the event sponsor, the Central Texas ACHE chapter would also like to thank these presenters for sharing their insights and best practices regarding healthcare data security. For more information on future events, please visit us at www.centraltexas.ache.org or send us an email at info@centraltexas.ache.org.