ICIT - Institute for Critical Infrastructure Technology

Key Issues in Rural Health Technology

As is well understood, of fundamental importance is the **availability of stable, reliable, and secure high speed Internet access** in rural areas. Unfortunately, Internet access continues to be a concern in many rural areas. Just as there was a need to put in phone service to each home, there is also a need to provide low cost Internet access to rural communities. Internet connectivity is now often a requirement in order to access medical services. For example, standard heart surgery protocol is to require the patient to weigh him or herself daily with a weight machine connected to the Internet as well as the doctor's office. If weight gains are outside the norm then action is taken on behalf of the patient.

Strong identity an access management for patient and medical professional access to EMR/EHRs is also crucial. Multi-factor authentication to ensure access only for those authorized and minimize identity theft must be widespread and commonplace in rural areas.

Interoperability of EMR/ERH is a major concern. The lack of interoperability causes errors in re-entry of data and lack of ability to leverage existing knowledge of the patient causes many tests to be redone.

Security of all medical devices is a major concern for all types of medicine, including rural. Most existing devices were not engineered from the beginning with security built in. Unfortunately, there are multiple examples of these devices being infiltrated.

Patient access to information is also necessary. The patient should have access to failure and success rates of medical devices, implants, hospitals and healthcare service providers.

HR 691 – Telehealth Modernization Act of 2015

ICIT Fellows have reviewed this legislation and advise the following principles and recommendations be kept in mind:

- The verbiage included provides for an overly basic definition of "Telehealth/Telemedicine." The current definition of the term is incomplete and should be expanded to include associated technologies.
- Further areas of specific concern that will need to be addressed as this bill is discussed include, but are not limited to:
    - Securing and protecting communication pathways used in the practice of Telemedicine/Telehealth. Explicit language should be included to specify an agreed upon level of security and encryption to be met during the medical use of Telephones, Cellular phones, VoIP calling (Voice over IP), Facsimile, Text/SMS/MMS, Video Conferencing, WebEx/Webinar, Online Chat/Online Video, and mobile applications.

  - Securing and protecting patient information and medical record data at rest, in-use, and in-transit during the practice of Telemedicine/Telehealth.
- Key principles for technology standards within the legislation should include:
  - Due to the wide and varied tastes of the general population, systems and applications used in the practice of Telehealth/Telemedicine should be required to be operating system and hardware/device agnostic.
  - National Licensure standards for Telehealth/Telemedicine providers.
  - Standards for reimbursement - Insurance, Medicare, Medicaid, and Private Payer.

Similarly, explicit language should be included to specify an appropriate level of security and encryption with regard to patient information, Electronic Healthcare/Medical Records, PII, and HIPAA data.

- This should not be limited to interactions between providers and patients, but should also specify the requirements to be met when these types of data are being stored, shared, and transmitted between Telemedicine providers of any variety (hospital, laboratory, pharmacy…etc).
- Providing secure access and authentication methods for both patients and providers, regardless of manner of access.

**Expert research contributed by the following ICIT Fellows*:

- William J. Billings (ICIT Fellow - Security Strategist, U.S. Public Sector, HP)
- Cynthia Cullen (ICIT Fellow - Security Strategist, Northeast, HP)
- Stan Wisseman (ICIT Fellow - Security Strategist, Southeast, HP)
- Chris Schumacher (ICIT Fellow - Sr. Technology Consultant, New Light Technologies)
- Dr. Kafi Wilson, MD – (ICIT Fellow – Doctor, KWMD LLC)
- Dan Waddell (ICIT Fellow - Director, Government Affairs, (ISC)2)
- James Scott (ICIT Senior Fellow – Institute for Critical Infrastructure Technology)
- Parham Eftekhari (Senior Fellow – Institute for Critical Infrastructure Technology)
- Morgan P. Muchnick (Senior Director of Legislative Affairs – Institute for Critical Infrastructure Technology)