Healthcare System's Weakest Link Impacts National Security

BOSTON *(December 3, 2019)* – Small and medium healthcare providers serve nearly 1 in 5 Americans, or over 75 million patients covered by Medicaid. Yet they represent the weakest link in terms of cybersecurity for our healthcare system, which has national security implications.

According to the FBI, healthcare is now the #1 target for cyberattacks. The Department of Health and Human Services (HHS) reports breaches are up 83% since 2010, and the true number of data breaches is far greater than what is reported to HHS. Nation states like China as well cyber criminals threaten not only individual patients, but our healthcare system as a whole. At the HIMSS Security Forum on December 10th, Health Tech Access Alliance will bring attention to how cybersecurity and HIPAA compliance challenges for small and medium businesses (SMBs) make achieving interoperability and securing our nation's healthcare system unrealistic until these risks are addressed.

"Security has often been a 'check the box' exercise. Small and medium size healthcare organizations for too long have believed that they would not be affected by cyberattacks and costly data breaches. They drastically underspend on data security and technology, and that makes our entire system more vulnerable. They are the weakest link in our nation's healthcare system in terms of cybersecurity," says Robert Zimmerman, Founder and President of Health Tech Access Alliance (www.htaalliance.org), a nonprofit member of Health Information Management Systems Society (HIMSS).

Mr. Zimmerman will be a featured speaker on center stage at the upcoming HIMSS Security Forum for a talk "Mission Critical: Securing Healthcare's Weakest Link" about the need to make security and HIPPA compliance simple, effective, affordable and realistic to avoid patient health records and personal information breaches. Most Americans do not realize health care records are up to 100 times more valuable on the dark web than Social Security and credit card information. Patients can find medical histories are compromised, and end up with medical bills for surgeries and services they never sought.

"To avert this threat, adequate training and attention to security and risk management for smaller and medium healthcare organizations is key. Community health centers, home health care, rural hospitals, long-term care facilities, and specialty clinics are all especially vulnerable. As healthcare providers adopt electronic health records, transition to integrated care, and provide patients with access to their own health records, the problem is escalating," according to Carol Loftur-Thun, Executive Director of HTAA.

HTAA will present results of a study on small and medium healthcare providers serving underserved communities. The study assesses cybersecurity vulnerabilities and shows industry baseline and trend lines to show the impact of interventions to improve cybersecurity and compliance. HTAA will outline lessons learned and "real world" recommendations, and Mr. Zimmerman will share his direct experience and stories from the front lines in working with SMBs in healthcare.

The HIMSS Security Forum is attended by senior healthcare administrators, compliance and privacy officers, healthcare directors, clinicians, and officials from government and academic institutions. The two-day forum features speakers and breakout sessions on information security recommendations and discussions with experts on cybersecurity risks and technology solutions to address gaps.

About HTAA

Founded in 2015, Health Tech Access Alliance is a nonprofit whose mission is to transform care for the underserved by empowering healthcare providers through access to technology, training, and solutions. We help providers protect patient privacy, improve health outcomes, and prepare for cyberattacks, emergencies, and disasters. HTAA staff have served with over 220 community health clinics, trained over 1,000 staff, and addressed thousands of cybersecurity vulnerabilities. HTAA's goal is to change the paradigm that training, security, and compliance must be costly or difficult. HTAA ensures small and medium-sized providers serving the underserved have access to knowledge and tools that larger, well-funded institutions enjoy.

###