LOK-IT
SECURE FLASH DRIVE™

## BACKGROUND

### UNIVERSITY OF TEXAS HEALTH SCIENCE CENTER AT HOUSTON (UTHEALTH)

The University of Texas Health Science Center at Houston is home to schools of biomedical informatics, biomedical sciences, dentistry, medicine, nursing and public health. UTHealth educates more healthcare professionals than any health-related institution in the State of Texas and features the nation's 7th largest medical school. UTHealth's 10,000-plus faculty, staff, students and residents are committed to delivering innovative solutions that create the best hope for a healthier future.

**If you would like to see how simple it is to deploy LOK-IT to secure medical records, we'd be happy to send you a LOK-IT in order to make an evaluation.**

**Executive Case Study:**

# LOK-IT and UTHealth

UTHealth™
The University of Texas
Health Science Center at Houston

### *Issue for UTHealth*: How to protect portable medical records

UTSD School of Dentistry students gain clinical skills at on-site clinics, affiliated hospitals and through community outreach projects. The school has affiliations with nine hospitals, 48 Houston Independent School District sites and more than 30 clinics, community agencies and long-term health care centers.

Because the students travel to the many clinics and community sites to perform dental care, the issue of patient record security posed a potential issue. If students were to learn from real-world dental work, a mechanism was required to transfer dental information for professors back on campus to provide input on the student's analysis and technique. USB flash drives happened to be the most convenient way for students to store the information for later access, but the federal government has strict regulations about portable data that are part of HIPAA (Health Insurance Portability and Accountability Act) requirements and the HITECH Act (Health Information Technology for Economic and Clinical Health Act). Among other topics, limitations are placed on removable devices, such as USB flash drives.

If patient data is lost or misplaced, healthcare entities and business partners must provide notification of breaches of health information and be subject to federal penalties unless the data is deemed Unusable, Unreadable, or Indecipherable to Unauthorized Individuals (UUI2UI). In regard to flash drives, there are basically three main requirements in order to meet this definition:

1. To achieve "safe harbor", the data must be rendered UUI2UI "through the use of a technology or methodology specified by the Secretary in guidance issued under [§ 13402(h)(2)]," which includes encryption with an algorithm consistent with NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices.
2. The encryption key should not be stored with the encrypted data, i.e. within the same flash memory. Stated within part (a) of the Guidance section- To avoid a breach of the confidential process or key, these decryption tools should be stored on a device or at a location separate from the data they are used to encrypt or decrypt.
3. To avoid the likelihood that protected health information would be stored on an unencrypted portion of a flash drive and assure that the data is UUI2UI, full-disk encryption should be utilized on the flash drive.

### *Solution*: LOK-IT Secure Flash Drive®

LOK-IT Secure Flash drives meet each of these three requirements. And, due to its platform independent, hardware user authentication design, not only did LOK-IT's security meet the HIPAA and HITECH regulations, but it also proved to be just as flexible as a standard USB flash drive. This was extremely important for the students as no standardized operating system was being used at the clinics in the field and the students themselves used different operating systems for their own laptops.

To ensure that LOK-IT is the only USB flash drive that is used in their internal dental school network, the IT department developed a simple port management control based on LOK-IT's model number. This ensures that UTHealth has no liability if a USB flash drive were to be lost. The only flash drives allowed are LOK-IT drives and if a LOK-IT were lost, the data is inaccessible and encrypted.

*Based upon DataLock®, licensed technology from ClevX, LLC – Patents Pending