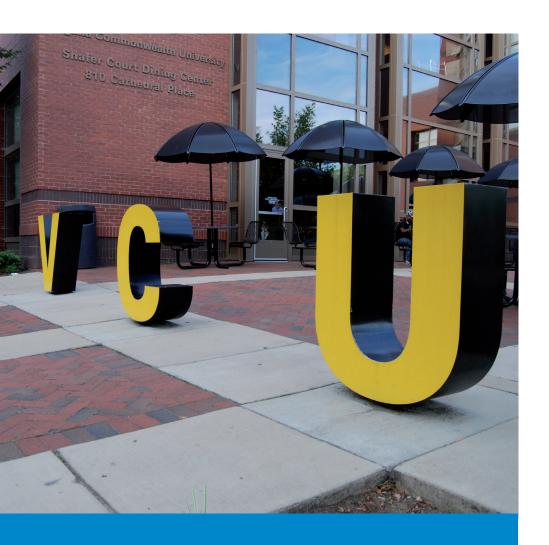# Healthcare and educational institution ensures compliance with data protection laws

Virginia Commonwealth University (VCU) deploys encryption solution on sensitive operational and medical data with minimal disruption to end-users

Business needs

VCU needed to encrypt multi-vendor desktops and laptops to ensure compliance with state and federal mandates for data protection with negligible end-user disruption.

Solution

After evaluating several products, the university chose to deploy Dell Data Protection | Encryption for its non-disruptive, flexible technology and superior customer support.

Benefits

- Uses a single encryption solution across an array of desktops and laptops
- Deploys transparently, with no end-user disruption
- Maintains end-user autonomy on a choice of devices
- Avoids pre-boot login authentication for end users
- Takes advantage of existing IT device investments
- Provides reporting to prove compliance with state and federal mandates

Solutions featured

- End point encryption
- Security

As a healthcare and educational institution as well as a major employer, the university must adhere to a variety of federal and state compliance mandates.

Virginia Commonwealth University (VCU), located on two campuses in Richmond, is known as one of the nation's leading medical schools and research institutions. With 33,000 students and 17,000 staff and faculty members — including physicians at the VCU Medical Center and its five health sciences schools — VCU provides care in more than 200 specialty areas. It is the region's only level-1 trauma center.

> Multi-device, multi-vendor support means staff can work on their preferred devices, increasing productivity and employee satisfaction.

University officials knew that compliance with all data protection laws—and protecting the institution's prestigious reputation—was critical. As a healthcare and educational institution as well as a major employer, the university must adhere to a variety of federal and state compliance mandates including:

- Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health (HITECH)
- Federally funded medical research, which is regulated under the Federal Information Security Management Act
- Student educational data, which is regulated by the Family Educational Rights and Privacy Act
- Faculty, staff, and student data, which is regulated under Commonwealth of Virginia laws

VCU faced a difficult challenge, after a security audit at the School of Medicine revealed they needed a way to encrypt data on a variety of desktops and laptops.

VCU's many educators, physicians and researchers have the autonomy to choose any type of desktop or laptop they want to use. The IT team needed to find a data protection solution that would:

- encrypt data in a multi-vendor, multi-platform environment
- avoid end-user disruption
- work with existing hardware devices

Data security on any device
The VCU IT team evaluated several data encryption products and found many lacking. Some did not have reporting they needed to verify that devices were encrypted. Self-encrypting drive (SED) solutions could not be deployed without replacing existing drives, which was cost-prohibitive. Software-based full disk encryption (FDE) solutions were also inadequate as they are not device agnostic and require time consuming pre-boot authentication.

The IT team implemented a pilot program to encrypt 30 laptops in the medical school's IT department with using the Dell Data Protection | Encryption solution (DDP | E). The laptops were encrypted successfully without a single failure, and most importantly, with no disruption to the end-users. Based on the success of this pilot, the IT team deployed DDP | E to 250 mobile PCs and 50 Macs in the medical school initially, followed by more than 2,000 additional licenses to various other medical school departments.

DDP | E is a single, cost-effective, manageable solution that can encrypt any fixed or mobile device from any manufacturer, including desktops,

Technology at work

Software
Dell Data Protection	Encryption (DDP | E)

laptops, tablets, smartphones and removable media devices. This makes it ideal for higher education institutions that work with devices from multiple manufacturers, and where disruption to normal operations is not an option.

Positive feedback from end users
VCU carried out a survey of end users and received resoundingly positive feedback about DDP | E. Most end users agreed that the product is not disruptive, and there was a high level of satisfaction across all employees surveyed. The excellent results of the satisfaction survey, combined with superior customer support from Dell, confirmed that DDP | E was the right solution to meet the university's unique data protection needs.

Effective compliance reporting
With DDP | E, the VCU IT team can produce reports to verify compliance with state and federal mandates and prove that endpoints were encrypted.

Maximum returns on existing hardware investments
With DDP | E, there is no need to replace laptops or other devices to encrypt them, so VCU can maximize on existing hardware investments. In addition, multi-device, multi-vendor support means staff can work on their preferred devices, increasing productivity and employee satisfaction.

Based on the success of its DDP | E implementation, VCU now plans to extend the solution to all faculty and staff devices across the university, ensuring that data security is never compromised.

> When the university tested the DDP | E solution on 30 laptops in the medical school IT department, it found that the technology was ideal for its needs.

View all Dell case studies at dell.com/casestudies

DELL