

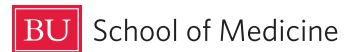
ePHI protection and VDI

John A. Meyers, Ph.D.

Assistant Professor of Medicine & Director of Technology



EXCEPTIONAL CARE. WITHOUT EXCEPTION.



Boston Medical Center is the primary teaching affiliate
of the Boston University School of Medicine.

Background

- Academic medical researchers often work with identifiable patient data for IRB-approved studies.
- Unlike EMR data, this data is often *unstructured* in the form of Excel sheets, Word documents, metadata in image formats, and sometimes as file and directory names themselves.
- An individual Excel file sometimes contains the names and medical information of thousands of patients!
- Faculty and staff often treat this data with the same care and concern that they give to their vacation photo collection due to lack of awareness of the regulations!
- Good intentions sometimes go very bad.
- **The average cost nationwide of a PHI breach in 2012 is \$2.23M.**

PHI SECURITY HAS KNOWN SOLUTIONS

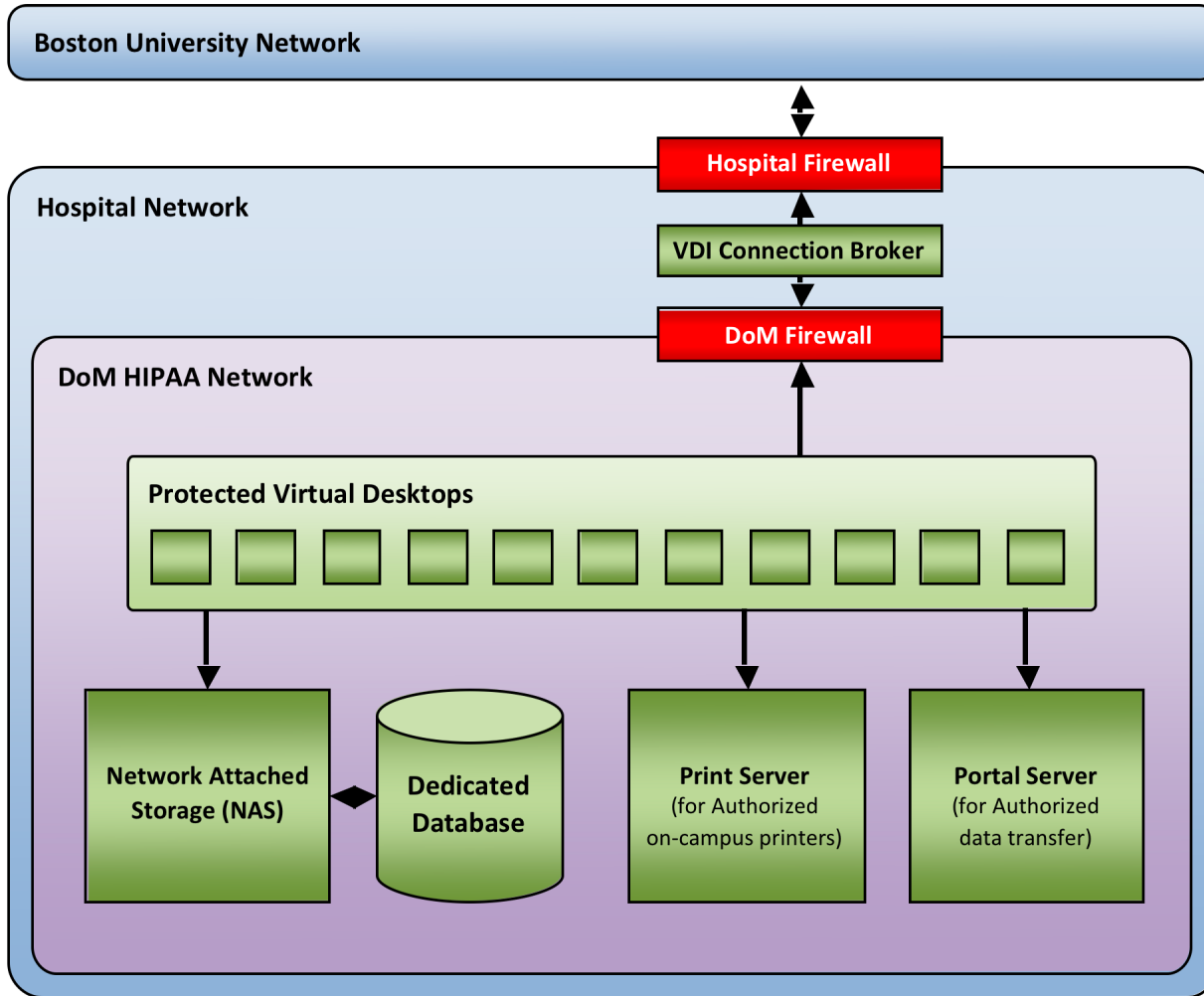
- Extensive guidelines, regulations, and best practices exist.
- Build a secure network. Firewalls and IDS at the edge. Inspect and restrict inbound and outbound traffic. Require device authentication to prevent BYOD scenarios.
- Lock down workstations. Prevent end-user software installation. Use cookie-cutter imaged desktops with extensive patch management and auditing.
- Lock down servers. Require two-factor authentication. Audit everything.
- Some large enterprises, and government, utilize an entirely separate “high side” secure network employing physical access segregation and isolation from intranet and internet.
- Install 2” steel door on office to keep rioters out.

THAT WON'T FLY IN ACADEMIA

- Before mentioned solutions are practical in commercial and government settings where there is strong administrative control.
- Academics are fiercely independent and by design are not subject to most HR and other administrative oversight.
- University networks are wide open and a BYOD culture is not only tolerated, it is expected and encouraged.
- Faculty choose specific hardware and software to address very specific scientific problems that IT may not understand or be aware of.
- Most data and processes are *not* subject to stringent regulatory controls. ePHI represents a small fraction of overall data.

OUR SOLUTION

- Build a completely self-contained high security environment that exists as a “bubble” within the larger untrusted academic network.
- Users can access this environment over VDI, but have no direct access to any of the components it contains.
- Therefore security and integrity of the environment is not dependent on end-user workstations and users are free to access the system from untrusted systems and locations knowing that the data itself *can not be removed from its secure bubble*.
- Requires users to consciously enter a separate environment re-enforcing that they are now working with sensitive data.



MAJOR COMPONENTS

- An internal network segment protected by a physical Cisco ASA firewall.
- A pool of linked-clone Windows 7 virtual machines on a Vmware vSphere 5 cluster.
- A Vmware View 5.1 connection broker server running as a virtual machine.
- A pair of Windows 2008R2 Active Directory servers as virtual machines hosting a stand-alone forest with no trusts to the primary “official” AD domains.
- A Solaris 11 NAS server utilizing the ZFS filesystem to provide storage to the virtual desktops.
- Two-factor, auditing, and print servers.
- Virtualization + blade technology = ~6U space

VMware View Client

Recycle Bin Token Management

desktop.ini

Windows DVD Maker
Windows Fax and Scan
Windows Media Center
Windows Media Player
Windows Update
XPS Viewer
Accessories
DNA Analysis Tools
Games
IBM SPSS Statistics
Maintenance
Microsoft Office
Mplus
PARSCALE 4.1
R
SAS
SharePoint
SSI, Inc
Startup
VMware
Winsteps

Meyers, John
Computer
Control Panel
Devices and Printers
Default Programs
Help and Support

Back

Search programs and files Log off

Start e File Explorer Media Player

5:47 PM
8/15/2012

Users can enroll their own Smart Phones as tokens

Standard Office productivity tools plus specialized scientific computing software

CLL patient data

Computer > Lerner (R:) > CLL patient data

Search CLL patient data

Organize Open Print New folder

File List:

Name	Date modified	Type	Size
CLL data sheet.doc	3/30/2012 4:28 PM	Microsoft Word 97 -...	31 KB
FrozenCLL.xlsx	3/30/2012 4:28 PM	Microsoft Excel Wor...	43 KB
Lauren Oshry's patients.docx	3/30/2012 4:28 PM	Microsoft Word Doc...	99 KB
Patients.xls	3/30/2012 4:28 PM	Microsoft Excel 97-...	21 KB
Thumbs.db	3/30/2012 5:52 PM	Data Base File	29 KB
VH Data CLL 706.doc	3/30/2012 4:28 PM	Microsoft Word 97 -...	41 KB

Context Menu:

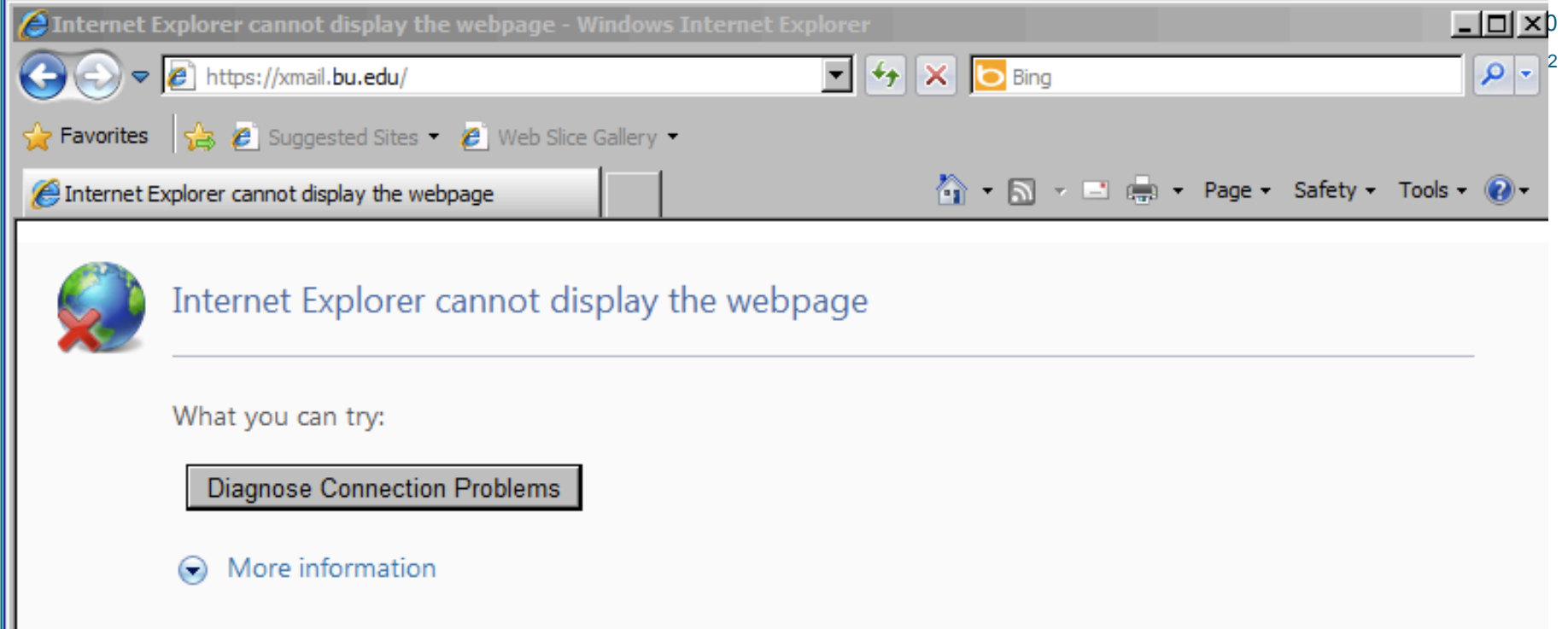
- Open
- New
- Print
- Open with...
- Restore previous versions
- Send to
- Cut
- Copy
- Create shortcut
- Delete
- Rename
- Properties

Annotations:

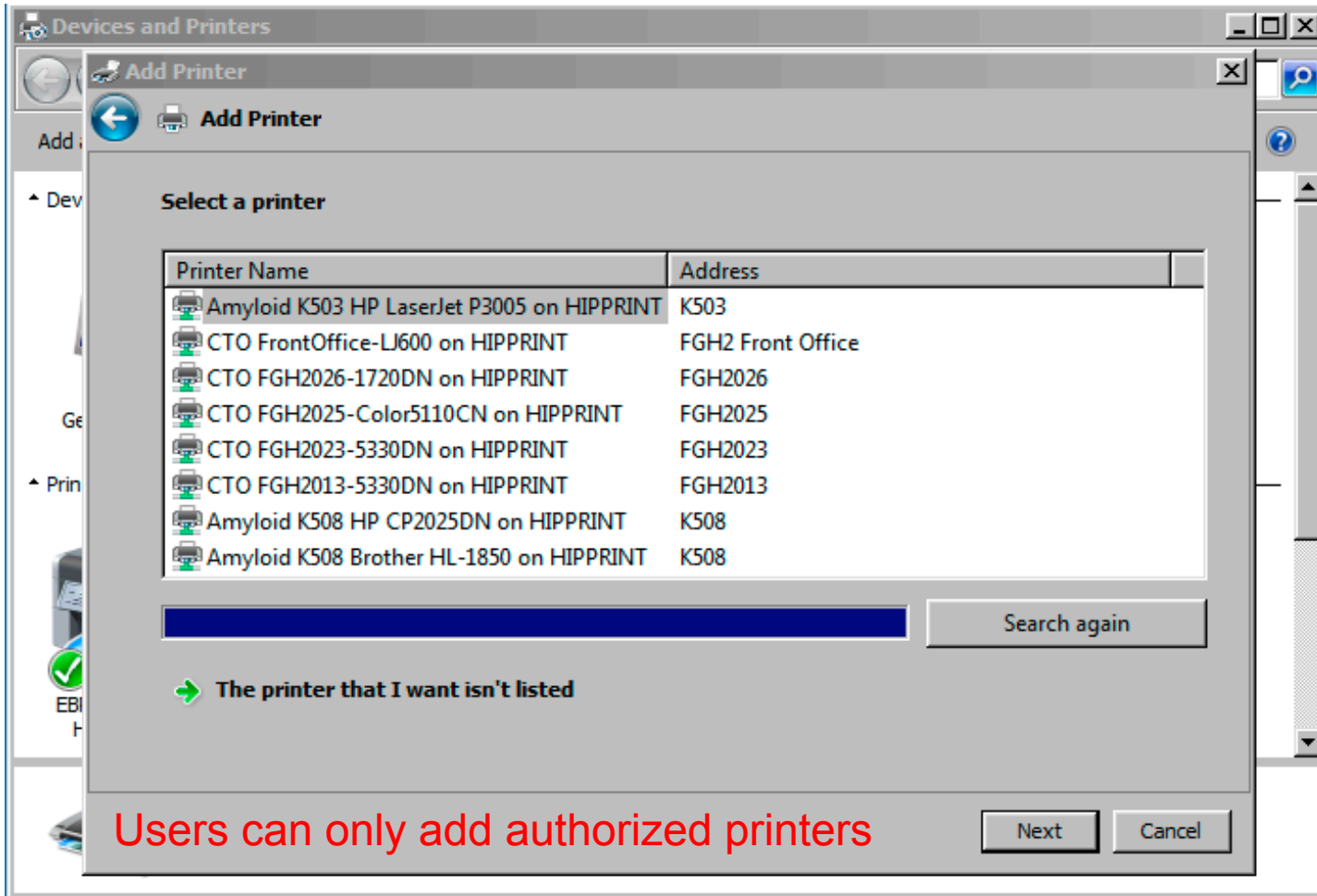
- PI's NAS share (points to Lerner (R:))
- \$2.3M file! (points to Patients.xls)
- Independent clipboard from client (points to Copy)
- Only way to copy data in/out (points to the context menu)

Taskbar:

Patients.xls Date modified: 3/30/2012 4:28 PM Tags: Add a tag
Microsoft Excel 97-2003 Worksheet Authors: Add an author



- The virtual desktops have no network access outside of the isolated network, not even to the University mail and web servers.
- This prevents copying of data without going through the one and only channel designed for that purpose.



Tracking code printed in microprint on all pages

Boston University Medical Center - Confidential - Printed Aug 15, 2012 6:06:01 PM (f3f1d4aac46d4d7eb2b9368d4ea4e656)

Portal (P:) [Window Title Bar]

Computer > Portal (P:) [Address Bar] Search Portal (P:) [Search Bar]

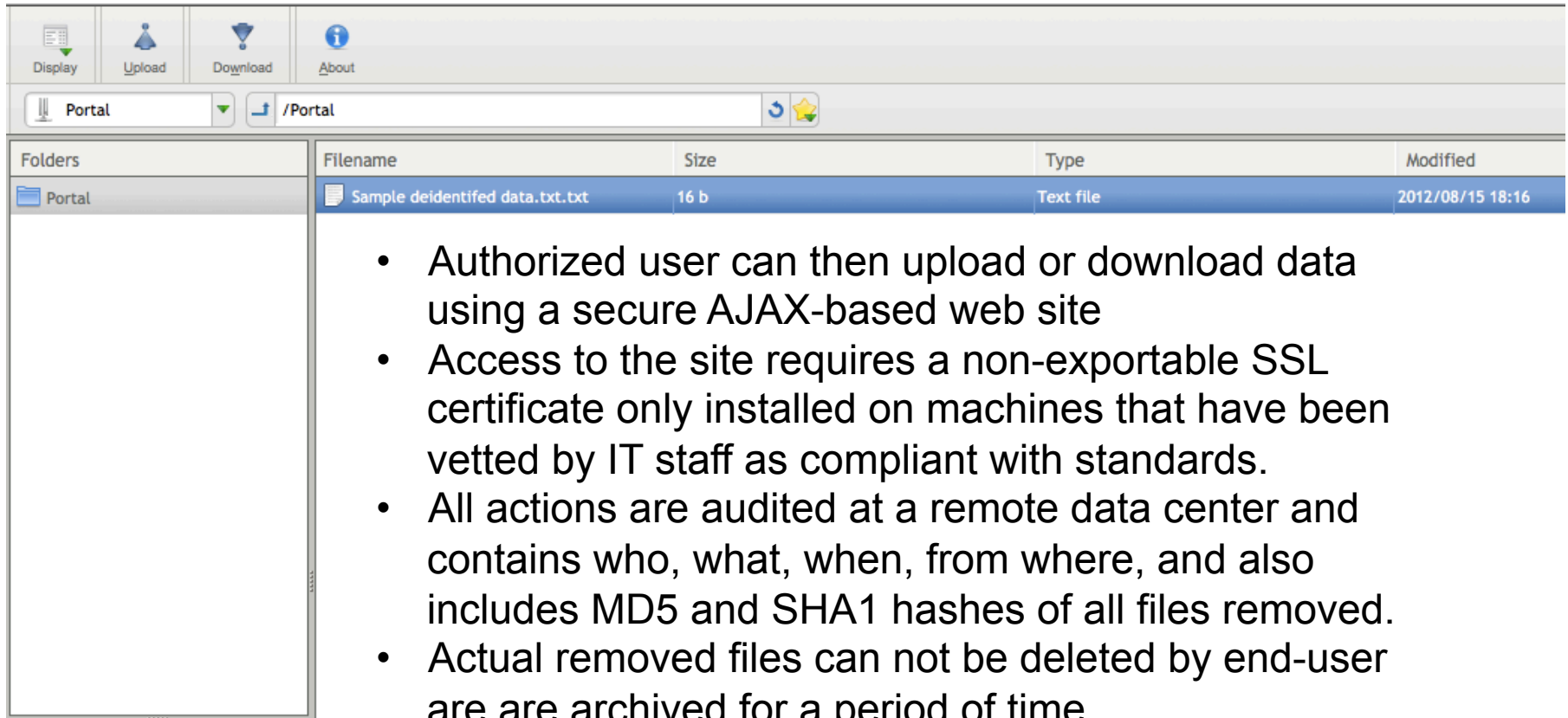
Organize Open Print New folder [Menu Bar]

Name ^	Date modified	Type	Size
Sample deidentified data.txt	8/15/2012 6:16 PM	Text Document	

To remove data, an authorized user copies the data to their personal Portal (P:) drive within the VDI and then proceeds to retrieve it by accessing a special website from their client PC.

Sample deidentified data.txt Date modified: 8/15/2012 6:16 PM Date created: 8/15/2012 6:15 PM
Text Document Size: 16 bytes

PORTAL WEB SITE VIEW

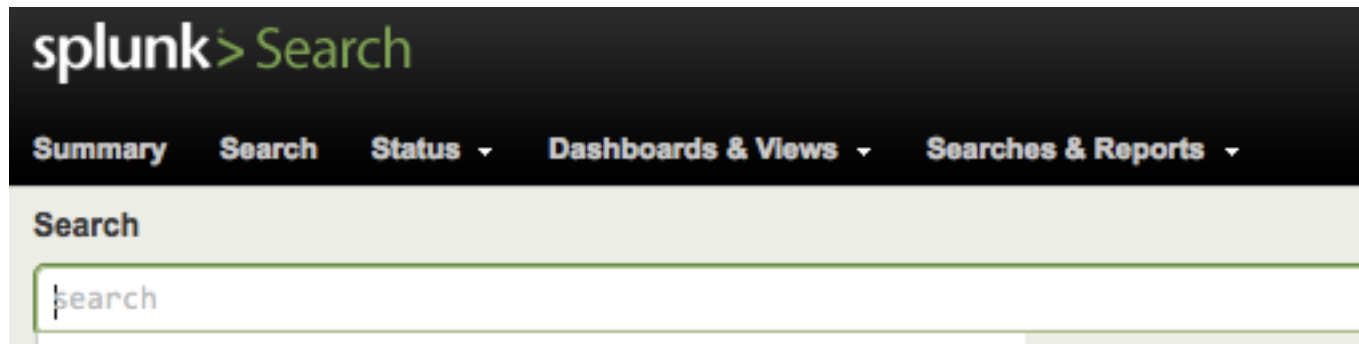


The screenshot displays a web portal interface. At the top, there are four buttons: 'Display', 'Upload', 'Download', and 'About'. Below these is a navigation bar with a 'Portal' dropdown menu and a '/Portal' address bar. The main content area is divided into two sections: 'Folders' on the left and a file list on the right. The file list has columns for 'Filename', 'Size', 'Type', and 'Modified'. A single file is listed: 'Sample deidentified data.txt.txt' with a size of '16 b', type of 'Text file', and a modification date of '2012/08/15 18:16'.

Folders	Filename	Size	Type	Modified
Portal	Sample deidentified data.txt.txt	16 b	Text file	2012/08/15 18:16

- Authorized user can then upload or download data using a secure AJAX-based web site
- Access to the site requires a non-exportable SSL certificate only installed on machines that have been vetted by IT staff as compliant with standards.
- All actions are audited at a remote data center and contains who, what, when, from where, and also includes MD5 and SHA1 hashes of all files removed.
- Actual removed files can not be deleted by end-user are are archived for a period of time.
- “Upload only” access level also available.

SIEM AUDITING AND LOGGING



- Single location with free text search allows access to all user and administrative actions auditing as well as firewall and IDS alerts.
- Dedicated Splunk instance exclusively for this environment and hosted in an off-site datacenter.
- Can free text search for user names, file names, hash values, dates, times, IP addresses, etc.

CONCLUSIONS

- Users were hesitant to adapt to a new system but once migrated reported that the performance of the VDI system was a huge plus, and in many cases was superior to their desktops.
- The conscience choice and isolated environment reminds users that they are working with sensitive data.
- Users also appreciate the relaxation of several desktop and server policies now that client machines no longer represent a significant threat.
- Several federal agencies including the SSA and NIH have reviewed and approved of our design for storage of low risk sensitive US government data sought for funded research.
- Most users report that the system is intuitive and does not disrupt work.

QUESTIONS?