3/16/2009

Notes/Review on Veteran Health Administration policy entitled:
RELEASE OF VA DATA TO STATE CENTRAL CANCER REGISTRIES
VHA DIRECTIVE 2007-023

- Policy effective 8/2007 to establish data release between VHA and State Central Cancer Registries
- Requires separate Data Transfer Agreement between VHA and each State
- Relys upon national standards for encryption, described by the National of Standards and Technology. Agency website is http://csrc.nist.gov/   (NOT to be confused with NIST.org)
- NIST certifies both approved technologies, AND specific products which are certified to implement these standards.
- While NIST approved technologies are included in specific products, VA requires that any encryption product (encryption modules) be explicitly approved and listed on the NIST list of approved products, which comply to the current standard called the Federal Information Processing Standards (FIPS) 140 designation. The standard is described at: http://csrc.nist.gov/cryptval/140-1/1401val.htm , and the specific list of approved products is maintained at http://csrc.nist.gov/groups/STM/cmvp/validation.html.
- VHA specifies in it's 2007 document that all data MUST reside in 'an encrypted partition on the hard drive and must be encrypted with FIPS 140 validated software'. (ie PGP Corp disk encryption tools)
- Current NIST validated FIPS modules list includes encrypted relational database products, which are certified to implement acceptable encryption modules. The list is located at: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm . This list includes major RDBMS including Microsoft SQL Server version 2008, Oracle version 8i and 10g. [note – does usage of these approved RDBMS supercede the necessity to also house the RDBMS data stores on a separately, encrypted partitions ?]
- Expressly forbids any 'redisclosure' of VHA data. Two classes of data transfer that are specified acceptable (and therefore NOT considered as 'redisclosure' are:

  o Submissions of de-identified VHA data to CDC / NPCR, NCI SEER, or NAACCR agencies.
  o Transmission of data with identifiers for linkage with other datasets to improve quality and completeness of reporting information. (examples include linkage with Indian Health Service, NDI, DMV agencies, voter registeration, etc)

-

Notes

Rich,

I should be available today after 2:00. My number here is 916-779-2567

Thanks,
Mike

Mike Warren
916-779-2567

Added to Dennis. They lost a lot of data, which prompted their guidelines.
NIST –

Truecrypt – uses approved TECHNOLOGY, but it's NOT on the 'vendor list' of approvals
http://www.nist.org/news.php?extend.167

Rich Pinder ❖ USC Keck School of Medicine ❖ *rpinder@usc.edu*
1420 San Pablo Street, Rm. B105 ❖ Los Angeles Ca 90033 ❖ Voice: (323) 442-1640 ❖ Fax: (323) 442-2485