

NIH Clinical Center CIO Newsletter

March, 2011

64th Edition

This is the sixty fourth edition of a monthly broadcast email to the CRIS user community about CRIS capabilities and issues. In addition to the text version in this email, I've attached a PDF version that can be printed. I look forward to receiving your comments or suggestions at CIOnewsletter@cc.nih.gov. In addition, valuable information can be accessed at the CRIS and DCRI websites: <http://cris.cc.nih.gov>, <http://www.cc.nih.gov/dcrl>.

Topics of the Month

- CIO Remarks
- Privacy and Security
 - New PIV Card Pin Reset Stations
 - Protecting NIH Network and IT Resources
 - Protecting Computers from Spam and Malware
- Tip for Using CRIS Sunrise
 - Updates to CRIS Research, Blood Order
 - Additions to Documentation of Consent
- New Reference Handouts

CIO Remarks: NIH Personal Identity Verification (PIV) Card Policy

Every system containing Personally Identifiable Information (PII) and/or sensitive data requires Homeland Security Presidential Directive 12 (HSPD-12) two-factor approved mechanism for login.

- PIV cards contain a secure digital certificate and require a PIN to authenticate.
 - You must know your PIN number. If you do not know what your PIN is, please go to the South Lobby Badging Station to reset it
- Because the CRIS system contains PII the PIV Card is an approved method for CRIS access.

Implementation for CRIS and CC Resources

By July 1, 2011

- NIH will use PIV Cards as the second factor for authentication for Remote Access.
 - CITRIX Farms, Remote Desktop, NIH VPN

- Every NIH networked computer **shall support** PIV card use (this requires PIV Card reader and software). This includes government owned and personally owned equipment.
- Effected computers include Mac and PCs, laptops and Blackberries – smart phones and cell phones are not practicable.

DCRI will provide updates monthly to CC staff.

New PIV Card PIN Reset Stations Coming

In the CIO Remarks you received an update on the deployment of PIV Card Readers in the Clinical Center. When DCRI desktop support staff install the PIV card reader and install the ActiveID software to your workstation or government issued laptop, you will be asked to test your PIV Card and enter the 6-8 digit PIN you specified when you picked up your ID badge.

Do you remember your PIN number? If not, you may bring your PIV Card to the NIH Badge Center located at the south entrance of the Clinical Center during business hours to be reset. For staff who work evenings, nights and weekends, DCRI is pleased to announce that the Systems Monitoring team in the CC datacenter can also reset your PIN. No appointment is required but we do ask that you call 301-496-7525 to let us know that you are coming. The CC datacenter is located at B25750 of the CRC.

DCRI will open a second PIN reset station in Bldg 10/2C262 in April. A third PIN reset station at Democracy II will open later in April. Look for details and contact information in future editions of the CIO Newsletter.

Protecting NIH Network and IT Resources

All staff and contractors need to be aware of a change at NIH that has been taken to protect the federal government IT resources and sensitive data contained in those resources. NIH Incidence Response Team (IRT) regularly scans NIH network traffic for the presence of Skype, IRC and Peer to Peer (P2P) software coming from internal IP addresses. P2P applications consume a disproportionate amount of resources. In addition, there are security concerns, and many of these P2P applications enable users to download computer viruses, Trojans or other computer malware. NIH has prohibited all P2P applications unless expressly authorized by a waiver from the agency.

Due to the increasing frequency of repeat offenders across all ICs and security risk to the NIH network, NIH began to automatically block IP addresses on March 14th if monitored traffic found “signatures” of Skype, IRC and P2P software.

Please review the list from IRT below. If any of these applications have been downloaded to your workstation or laptop, please remove them immediately. If your IP address is blocked, the IRT will not unblock the IP address until it has been removed and validated by the security team. If you have questions, please contact the security team at CC-ISSO@cc.nih.gov

HTTP: Skype Call-To Buffer Overflow
IRC: IRC Client Activity Detected
P2P: Ares/Warez-Gnutella Traffic Detected
P2P: Azureus Traffic Detected
P2P: BearShare Alive
P2P: BitTorrent File Transfer Handshaking
P2P: BitTorrent Meta-Info Retrieving
P2P: DC (Direct Connect) Traffic Detected
P2P: eDonkey Traffic Detected
P2P: Gnutella Traffic Detected
P2P: KaZaA Client Connecting to Server
P2P: KaZaA File Transferring
P2P: Kugoo Traffic Detected
P2P: LimeWire Alive
P2P: Manolito Protocol File Search Detected
P2P: Morpheus Alive
P2P: Octoshape Traffic detected
P2P: Pando Traffic detected
P2P: Peer-to-peer Distributed File Download Obfuscated-Traffic Detected
P2P: PPLive Traffic Detected
P2P: PPStream Traffic Detected
P2P: QQDownload Traffic Detected
P2P: QQLive P2P Streaming Media Detected
P2P: QQLive Protocol Detected
P2P: Shareaza Alive
P2P: Skype Logon Process Detected
P2P: TeamViewer Traffic Detected
P2P: Thunder KanKan Traffic Detected
P2P: Torrent uTP BEP-29 Traffic Detected
P2P: WinMX Traffic Detected
P2P: Xunlei Traffic Detected
SSH: SSH Login Bruteforce Detected

Protecting Computers from Spam and Malware

Everyone uses a web browser to access the Internet which makes the web browser a target for bad actors that want to install malicious software, or “malware.” In the past, users had to take specific actions, like opening an email attachment, for their computer to become infected. Today, simply visiting a website can cause your computer to become infected. This is called “drive-by-

download.” Features built into web browsers that allow them to run scripts, like display a video, or maintain a shopping cart, can also be used to install malware on your computer without your knowledge or consent.

What can you do to protect your privacy and your computer and keep your browser safe? Listed below are some general browser security tips.

- Keep your browser up-to date. Running the latest version of your browser ensures that you have the benefit of the latest security technology. Make it a habit to check that your browser and plug-ins are up-to-date each month.
- Be careful about browser plug-ins. Plug-ins are small downloadable programs that add functionality to your browser. When you browse to a website, you may receive a message onscreen that in order to work with the site, you have to download and install a browser plug-in. “Just click here” sounds innocent but “think before you click.” Remember any program you install will need to be updated, and may contain security vulnerabilities. Do you know the website and the plug-in are trustworthy? The fewer plug-ins you have installed, the safer your browser will be.

Updates to CRIS Research, Blood Order

The CRIS Research Blood order form has been updated to include the following functionality. These changes were placed in Production CRIS on March 17th.

- Some research blood draws involve labels generated from the CRIS barcode system as well as labels provided by the research team. Fields have been added to capture both of these values which are used to calculate a total number of labels.
- The Maximum Blood Draw Volume field is calculated based upon the tube size selected and the total number of labels (applied to tubes) involved in the blood draw. For example, if the tube type is ACD Yellow, the tube size is 8.5 ml. If 3 labels will be generated from CRIS and 2 labels will be provided by the research team, then the maximum volume is $8.5 * (2 + 3) = 42.5$ ml.
- A Total Blood Draw Volume field has been added to indicate the total desired volume of blood to be drawn in all of the research tubes. This value cannot exceed the Maximum Blood Draw Volume.
- A calculated Blood Draw Volume Per Tube field has been added to indicate the amount of blood volume to draw in each tube. This is calculated based on the Total Blood Draw Volume divided by the total number of labels applied to tubes. If the Total Blood Draw Volume is not to be divided equally among the tubes, the exact volumes should be indicated in the Special Instructions field.

DLM_ResearchCollectBlood2 - SPRINGSTART, PATC NMN

Research, Blood - SPRINGSTART, PATC NMN

Order: Research, Blood Order ID: 002BGG049

Requested By: Carlson, Seth Template Name:

Messages: Research, Blood tube types are now differentiated.

Requested Collection Priority: Routine Collect Specimen On: 03/09/2011 View DLM Website:

Research Instructions: Enter total amount of blood to be collected in all tubes in Total Blood Draw Volume (ml) field. Select the button above to view the DLM website for different tube types. If selecting Other (MSC), enter specific tube type in Special Instructions.

Test Name: Research Research Tube Additive: ACD Solution A

Type Of Tube: ACD Yellow (HLY) Total Blood Draw Volume (ml): 25 Maximum Blood Draw Volume (ml): 42.5 Blood Draw Volume Per Tube (ml): 5

Label Instructions: Enter the number of tubes to be collected through the CRIS Barcode system in the Labels from CRIS field. If there are additional labels supplied by Research Team, enter them in the Labels from Research Team field for the calculation of Max Blood Volume.

Number Of Labels From CRIS: 3 Number Of Labels From Research Team: 2 Total Number Of Labels: 5

Tube Size (ml): 8.5

Alternate Printing Note: Specimen collection and label printing will occur at the patient's registered clinic/unit location at the time the specimen is due to be drawn. If you want specimen collection and label printing to occur elsewhere, indicate location in the field below.

Specimen Collection/Label Printing Site:

Special Instructions: RN to use labels from CRIS CareFusion Barcode in addition to labels provided by Research Team. Total number of labels = 3 from CareFusion + 2 from Research Team for a total of 5 labels.

Item Info Repeat View Document OK Cancel

Additions to Documentation of Consent

At the request of the Rehabilitation Medicine Department, two observations will be added to the Protocol identification section of the Progress Note – Documentation of Consent document the first week of April. They are “Date of Enrollment” and “Consent Obtained By”. And you can use the Modify Template button to add a section for Re-Consent documentation.

Re-Consent

- Inclusion and exclusion criteria were reviewed and the subject is still eligible to participate
- The subject was reconsented with an updated consent form

New Reference Handouts

The following two reference handouts were developed due to recent and increased inquiries on the subject matters:

1. Author By Feature: Used to Enter Documentation on Behalf of Another Provider
2. How to become a CRIS User.

They can be found on the CRIS webpage → Reference Materials:

<http://cris.cc.nih.gov>