

NIH Clinical Center CIO Newsletter

May, 2011

66th Edition

This is the sixty sixth 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

- New in CRIS
 - Specimen Collection Status
- Privacy and Security
 - Security Awareness Refresher Course
- CRIS Support
 - CRIS Downtime
- 2 Factor Authentication

Checking Status of Specimen Collections in CRIS

We'd like to report a huge enhancement to reporting the status of specimen collection in CRIS.

- When a specimen collection order is released/activated, the lab order will update to "*Pending Collection*" on the CRIS Orders tab.
- When you scan your specimen as collected in CareFusion, the lab order will update to "*Specimen Collected*" on the Orders tab. For more information, right-click on the order's History Status to view the exact date/time collected. In the example below, line item #204 displays "*Collected, HL7 Interfaces*" in the "Who Requested" column.
- When the specimen is received in DLM, the lab order will continue to reflect "*Specimen Collected*" on the Orders tab. You can obtain information on the received status by right-clicking on the order's History Status to view the exact date/time received. In the example below, line item #205 displays "*Received, HL7 Interfaces*" in the "Who Requested" column.
- When the lab results have posted to CRIS, the lab order will update to "*Final Results*" on the Orders tab. For more information, right-click on the order's History Status to view the exact date/time resulted. In the example below, line item #206 displays a resulted date/time of 5/11/2011 @ 07:47; the ordering physician's name typically displays here.

ID	Function	Signed	When	Who Entered	Who Requested	Source
201	New		05/10/2011 18:45	Shah, Syed A (MD)		
202	Acknowledged		05/10/2011 19:25	Renzsch, Christina M (RN)		
203	Auto Activated		05/11/2011 00:15	ORDER STATUS UPDATE BATCH (MD)		
204	Specimen Received		05/11/2011 05:54	Interfaces, HL7 (IT)	Collected, HL7 Interfaces (IT)	
205	Specimen Received		05/11/2011 06:59	Interfaces, HL7 (IT)	Received, HL7 Interfaces (IT)	
206	Resulted		05/11/2011 07:47	Interfaces, HL7 (IT)		(MD)

Security Awareness Refresher Course

Reminder - The 2011 Information Security Awareness Refresher Course must be completed at the Training Website by June 15th

Failure to complete this training by the deadline means that your Active Directory account will be disabled.



Directions for Taking the 2011 Refresher Course:

- Where is it? Go to the Training Website at: <http://irtsectraining.nih.gov/>. Log in with your NIH ID and select the 2011 Refresher.
- Highlights of the training include a lead-in segment on Phishing, updated screens, and four new screens addressing: Two-Factor Authentication, Mobile Device Security, Fake Anti-Virus and Personally Owned Equipment.
- **Beginning this year, there are TWO versions of the Refresher.**
 - Most of you will see the regular version of the Refresher.
 - If your IC considers you to be a “Privileged User”, you will see a slightly longer version of the Refresher that includes a few extra training screens and an additional *Rules of Behavior for Privileged User Accounts*. If you have local administrator access to your computer, or elevated access privileges to an IC or NIH system, you’ll be seeing the extended version of the Refresher.
 - The training system will give you the appropriate version based on your NIH ID, i.e., when you log in, the system checks to see if your ID was tagged as being a Privileged User. No tag means you see the regular version.
- Why did we create two versions? When HHS revised their [Rules of Behavior](#), and added the new annual requirement that staff designated as a “Privileged User” must also agree to [Rules of Behavior for Privileged User Accounts](#), we decided that it would be better for those affected by this change to get two mandatory training requirements done at the same time!



If you have any technical problems taking the course, please contact the NIH IT Service at <http://itservicedesk.nih.gov/>.

Any questions concerning this request should be directed to the CC ISSO at CC-ISSO@cc.nih.gov

CRIS Downtime

Over the past year DCRI, in conjunction with other clinical and ancillary departments, have been addressing how to improve the communication and education of CRIS downtime processes and procedures. As a result, many positive changes have and will be taking place.

New Manual Downtime forms

Some of the older downtime manual forms will no longer be used (e.g. Medical Records/ Doctor's Orders -SF508). A Downtime forms committee has revised as well as created some new downtime manual forms. These forms will be available through the Medical Record Department.

Downtime Toolkits

Over the next few weeks, all patient care areas will receive downtime toolkits. Downtime Tool Kits contain the new CRIS Downtime Manual forms and reference handouts. They will be centrally located and available in all patient care areas for use during downtimes. Each area is expected to maintain/restock their tool kit as needed and may contact the Medical Record Department to replenish supplies.

CRIS Sundown

Whenever there is an extended CRIS Sunrise downtime greater than **90 minutes**, an application called CRIS-Sundown will be made available to users. CRIS Sundown is a copy of the current CRIS Sunrise with view only and printing capabilities. The CRIS Sundown Icon is accessed through Citrix at <https://cccasper.cc.nih.gov>.

Additional downtime information is available on the CRIS web site <http://cris.cc.nih.gov/procedures/downtime.html>

2 Factor Authentication

What's Happening: The NIH CIO has mandated that the NIH transition to 2-factor authentication for Remote Access NIH VPN by July 1, 2011. The purpose of this transition is to satisfy a security finding that has been long outstanding and to improve NIH's information security posture. The use of 2-factor authentication requires the person logging on to the NIH Network to have two independent items of authentication such as;

- Something that the person has like a PIV card (NIH badge)
- Something that the person knows like the PIN associated with the PIV card

Who's Affected: All users of the NIH Remote Access NIH VPN and users of CC CASPER, CRIS-Sunrise, ESA or any NIH Resources from non NIH locations.

What Do I Need to Do: In order to be prepared to utilize your PIV Smartcard for 2-factor authentication the following must be in place:

1. If you have **Government Furnished Equipment (GFE)**, you will need a PIV Smartcard (NIH badge) reader for the computer. If you do not have a PIV Smartcard USB reader built in, then one will be provided by DCRI for Government furnished laptops.
2. If you have **Government Furnished Equipment (GFE)**, you will need the new Cisco AnyConnect NIH VPN client installed.
 - DCRI User Support will contact you directly to have your Government Furnished laptop brought in to perform a laptop health check. At which time the new AnyConnect VPN client, PIV card reader ActivID software and drivers will be installed onto your GFE laptop.
3. If you have **Personally Owned Equipment (POE)** you will need a PIV Smartcard USB reader, PIV card and ActivID software installed on your **Personally Owned Equipment (POE)**.
 - o To access the instructions for installing ActiveID client software and configuring PIV certificates click on the following link: http://smartcard.nih.gov/PKI_PIVguides.htm. If you experience any issues please contact the NIH IT Service Desk at 301 496-4357.

- o For information about where to purchase PIV Smartcard USB readers located under Supported USB devices for **Personally Owned Equipment (POE)**.
 - o If you use the NIH VPN you will need the new Cisco AnyConnect NIH VPN client installed. Instructions for installing the new Anyconnect VPN client are available at <http://isdp.nih.gov/isdp/version.action?prodid=140>
4. You need to know the PIN associated with your PIV card. You created this PIN when you first received your PIV card. If you don't remember your PIN, follow the instructions below to have your PIN reset.

How Do I Test My PIV Card: Note: The following steps allow users to test the PIV card reader, PIV PIN from non NIH location

1. Insert PIV card into their PIV/smart card reader
2. Go to <https://ned.nih.gov/ned> and click on the "Log in" button on the RIGHT HAND SIDE of the page

Getting your PIV PIN reset:

- Please go to the South Lobby Badging Station in Bldg 10 to reset it.
- For staff who work evenings, nights and weekends, the CC datacenter can reset your PIN. No appointment is required but we do ask that you call 301-496-7525 prior to coming. The CC datacenter is located at B25750 of the CRC.

Supported USB devices for Personally Owned Equipment (POE):

SGT111 DOD Military USB Common Access CAC Smart Card Reader
\$26.00

http://www.amazon.com/SGT111-Military-Common-Access-Reader/dp/B003HI83WO/ref=pd_bxgy_e_img_b

SCM Microsystems USB Smart Card Reader (SCR3310) **\$16.99**

http://www.amazon.com/Microsystems-Smart-Card-Reader-SCR3310/dp/B0012K5P02/ref=pd_sim_e_4

SCM SCR331 USB Common Access CAC Smart Card Reader, CCID Compatible for Windows 7 Vista XP Mac and Linux Computers **\$14.49**

http://www.amazon.com/SCM-SCR331-Compatible-Windows-Computers/dp/B002XJG71M/ref=pd_sim_e_3

SGT118 Smart Badge CAC ID Holder & USB Smart Card Reader **\$34.95**
http://www.amazon.com/SGT118-Smart-Badge-Holder-Reader/dp/B003V8TFEA/ref=pd_sim_e_8

If a user would like to check to see if they have a compatible USB smart card reader for windows 7 32 & 64

<http://www.microsoft.com/windows/compatibility/windows-7/en-us/Browse.aspx?type=Hardware&category=Graphics%20Cards%20%26%20Components&subcategory=Smart%20Cards&page=2>

If you have any questions or would like for us to attend a Departmental meeting to review with your staff then please contact Yvonne Almazan, yalmazan@nih.gov.

DCRI ROAD TRIPS

On May 6th, DCRI participated in the Healthcare IT Roundtable, a quarterly event held at Penn Medicine in Philadelphia. It is comprised of various health systems and includes collaborative discussions, knowledge sharing, innovative demonstrations, and brainstorming. Dr. Patty Sengstack, Deputy Chief Information Officer (CIO), [Clinical Informatics](#), and Dr. Jon Walter McKeeby, CIO, NIH/CC, co-presented “Project Prioritization at the NIH Clinical Center”. Susy Postal, Team Lead for Support, Training, and Analysis, presented “Supporting System Downs: DCRI’s Downtime Procedure”. It was a wonderful opportunity for DCRI to participate, contribute, and learn from other facilities.

On May 12th-14th, at the American Nursing Informatics Association (ANIA-CARING) Annual conference, Sue Houston, Chief, Portfolio and EPLC Management, and Patty Sengstack presented the following:

1. “A Two-Phased Approach to Evaluate the Success of HIT Implementations”
2. “Project Management: The Next Level – Managing Scope, Risks & Issues”
3. “2010 Year in Review of Informatics Research - Pre-conference Workshop”

NIH Research Festival May 18

Jackie Feinberg, a post-bac IRTA for DCRI over the last year, presented pilot work she has done with documenting MLM's in CRIS, one strategy to improve clinical documentation.



Take Your Child to Work Day

DCRI participated in Take Your Child to Work Day held Thursday April 28th. Two sessions offered a total of 23 children and their parents/guardians who learned about networks and dissected a computer.

