..CONNECTIONS NEWS..

for the week of December 12 - 19, 2008

Developing a more caseworker centric system

CONNECTIONS Intranet site: http://ocfs.state.nyenet/connect/

FEATURED IN THIS EDITION

"Info to Know" for Caseworkers

- *CONNECTIONS Records Retention Notification: Program Purge Scheduled for Monday, December 15th …pg. 1 …more*
- *UPDATE Reminder about Permanency Hearing Reports …pg. 2 …more*
- *OCFS Data Warehouse News: Revised Version of the Children Served with Missing Clinical Diagnosis (LDSS) Report - New Report for Voluntary Agencies the Children Served with Missing Clinical (VA) Report …pg. 3 …more*
- *Two NEW CONNECTIONS Tip Sheets - The Family Assessment and Services Plan and the Permanency Hearing Report Procedure …pg. 4 …more*

General "Info to Know"

- *CIO/OFT Notification 08-CNS-11 Microsoft SCCM Implementation …pg. 4 …more*
- *NYS Office of Cybersecurity and Critical Infrastructure Coordination Information Bulletin ..pg. 7 …more*
- *NEW Postings to the CONNECTIONS Intranet … pg. 8 …more*
- *Weekly System Maintenance … pg. 8 …more*

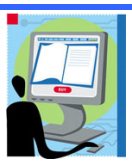
"Info to Know" for Caseworker

CONNECTIONS Records Retention Notification: Purge Program Scheduled for Monday, December 15th

Please note that this notification is for local district staff only.

This information has been included in the previous two editions of the CONNECTIONS NEWS and was sent as an individual communication to designated local district staff that performs this function.

The next Records Retention Purge Program is scheduled to begin ***Monday evening, December 15, 2008***. This program will purge cases/stages listed in the **September 15, 2008** "To Be Expunged" report. Please note that if you have not already reviewed and made the necessary demographic changes, via Local Data Maintenance, to the cases/stages identified in the September "To Be Expunged" report you have until close of business on *Sunday, December 14th* to do so.



UPDATE **Reminder** *about Permanency Hearing Reports*

This information was included in the previous edition of the CONNECTIONS NEWS .

The fix that was implemented in Build 18.10.3 limited the chances for **future** corruption in the PHR as a result of an unexpected text control error when attempting to re-open a *Permanency Hearing Report (PHR)* after information had been recorded and saved as draft or final.

Please note: The fix applies only to PHRs that were started *after* 11/22/08 (after the implementation of Build 18.10.3). Efforts are currently underway to address issues in PHRs that were launched *prior* to 11/22/08.

If you encounter errors and are unable to access a DRAFT PHR, in order to continue work in the PHR please follow the steps below:

If you encounter errors and are unable to access a DRAFT PHR, in order to continue work in the PHR please follow the steps below:

- Highlight the DRAFT PHR IN CONNECTIONS
- Click on Options; Mail Local Copy; Permanency Report, which will prompt CONNECTIONS to send the DRAFT PHR to you (as the logged on user)
- Delete the original DRAFT PHR within CONNECTIONS (Please make sure not to delete the PHR within CONNECTIONS until after you have had CONNECTIONS send a copy of it to you.)
- Launch a new PHR within CONNECTIONS and use the no-prefill option
- Open the DRAFT PHR in your email and copy and paste the information from the DRAFT PHR to the PHR that you just launched in CONNECTIONS
- Double delete the Draft PHR in your email

If you need further assistance, please contact the Application Help mailbox. The address of that mailbox is: ocfs.sm.connections_app_help. (Please note that there are two underscores in the address. If you are emailing 'out of our network' we ask that you add the following piece to the address: @dfa.state.ny.us or, @nysemail.state.ny.us.)

OCFS Data Warehouse News…

- *Revised Version of the Children Served with Missing Clinical Diagnosis (LDSS) Report*
- *New Report for Voluntary Agencies: the Children Served with Missing Clinical Diagnosis (VA) Report*

The OCFS Data Warehouse has released a revised version of the *Children Served with Missing Clinical Diagnosis (LDSS)* report. In addition, there is a new report for Voluntary Agencies: the *Children Served with Missing Clinical Diagnosis (VA)* report. These reports list children who have not had a health checkup. The LDSS version only includes cases where the Case Manager is from the District selected at the prompt. The VA version only includes cases where the Case Planner is from the Voluntary Agency selected at the prompt. Both versions are in Cognos 8 and can be accessed via the following path:

Public Folders > Global Reports > OCFS > Data Warehouse Reports > AFCARS Reports

Please note that the Case Manager's Office and Unit have been added to the LDSS version. The VA version contains the Case Planner's Office and Unit.

The reports provide detail information for:

LDSS version	VA version
Case Manager (name)	Case Planner (name)
Case Manager Office	Case Planner Office
Case Manager Unit	Case Planner Unit
Case Planner Agency Id and Name	Case Manager Agency Id and Name
Case Planner Name	Case Manager Name

Remaining columns for both versions

CCRS Case Id	Stage Id
CONNX Case Id	Stage Start Date
Case Name	Stage End Date
Child CIN	Health Responsibility Agency
Child Id (Person Id)	Health Responsibility Start Date
Child Name	Health Responsibility end Date

Both reports have a "Sort by" Option.

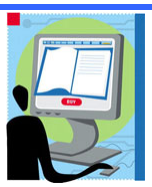
LDSS version:

The default sort order is by Case Manager.
Choices include: Case Manager, Case Planner Agency, Case Planner, CCRS Case ID, Child CIN, Child Name, and Health Responsibility Agency

VA version:
The default sort order is by Case Planner.
Choices include: Case Planner, Case Manager Agency, Case Manager, CCRS Case ID, Child CIN, Child Name, and Health Responsibility Agency

- *UPDATE on the FASP Due Calendar Report*

We are pleased to announce that the FASP Due Calendar Reports (LDSS & VA), that were previously disabled, are now available for use.



Two NEW CONNECTIONS Tip Sheets - The Family Assessment and Service Plan and the Permanency Hearing Report Procedure Tip Sheets

This information was included in the previous edition of the CONNECTIONS NEWS .

CONNECTIONS Tip Sheet - The Family Assessment and Service Plan

The Family Assessment and Service Plan tip sheet provides an overview of the FASP, and describes the types of FASPs and timeframe, how to modify a FASP component after it has been launched, how to perform the removal update process, how to perform the FASP pre-launch tasks, how to determine who will record what is in the FASP, as well as a description of the FASP submission process. The tip sheet is posted to the CONNECTIONS intranet website and can be accessed by clicking on the following link: http://ocfs.state.nyenet/connect/jobaides/Tip%20sheets/FASP%20Tip%20Sheet_v1%200%20WEB.pdf

CONNECTIONS Tip Sheet - Permanency Hearing Report Procedure

The Permanency Hearing Report Procedure tip sheet provides information about how to decide which type of PHR to launch, how to review and verify case information, how to decide whether to pre-fill the report, how to review and update outside participants, how to launch the Permanency Hearing Report and how to finalize the Permanency Hearing Report. The tip sheet is posted to the CONNECTIONS intranet website and can be accessed by clicking on the following link: http://ocfs.state.nyenet/connect/jobaides/Tip%20sheets/Permanency%20Hearing%20Report%20Procedure%20Tip%20Sheet%20v1.0%20web.pdf

General "Info to Know"

CIO/OFT Notification 08-CNS-11
MICROSOFT SCCM IMPLEMENTATION

NUMBER: 08-CNS-11
TITLE: MICROSOFT SCCM IMPLEMENTATION
DATE ISSUED: December 9, 2008

Please note that the following information is pertinent to district and agency LAN Admin and IT staff.

Description of the Impact

Effective December 15, 2008, Microsoft System Center Configuration Manager 2007 (SCCM) will replace Tivoli Configuration Manager, Tivoli Remote Control, and Microsoft WSUS as the workstation management solution for CNS supported workstations.

The most significant change for LAN Administrators and Agency IT staff will be the shift to Microsoft SCCM Remote Control and Remote Desktop. For authorized users, Remote Control Access will be available at http://wsushsen0a1ab.hsen/RemoteControl. SCCM Remote Control will introduce three key improvements, which have been requested by several CNS customers:

- Improved performance–SCCM Remote Control uses the RDP protocol, which is optimized to work with limited bandwidth.
- Improved remote control acceptance–Users will now be aware of the identity of the user connecting to their workstation.
- The ability to securely access workstations (XP only) without user input. If an end user is logged out or has the screen locked, SCCM allows an administrator to force the user to log off (if a workstation is locked) and log in with administrative credentials.

Other impacts of this SCCM Implementation Phase will include "behind the scenes" changes to software distribution, patch management, and configuration management. These changes will improve CIO/OFT's ability to manage workstations, but will not directly impact LAN Administrators or Agency IT staff.

Instructions for Setting up SCCM Remote Control Icon

For authorized users of remote control, copy and paste the remote control shortcut \\sofhsen0a1aa\Softshare\RemoteControl to your desktop. If this does not work, right click and hold while dragging the link to your desktop. You will see an Internet Explorer icon on your desktop with the caption "Remote Control."

1. The above link will prefix **"ADM"** to whatever user ID you are currently logged in with, and will launch Internet Explorer with those credentials. If you are not logged on with the HSEN ID you want to use, you will need to modify the shortcut manually. (If you are logged in with the desired ID, steps "a." and "b." are not necessary.)

    a. To do this, right click, choose Properties, and go to the Shortcut Target Path. Change "adm%username%" to the appropriate ADM credentials.

    b. Click OK, and you are ready to launch Remote Control.

2. You will need to add the site to your **Trusted Sites** list in Internet Explorer. To do this, after you have launched the web shortcut, click Tools\Internet Options\Security Tab. Select "Trusted Sites" from the "select a zone" box at the top and click the "sites" button just below it. Make sure "require server verification (https:) for all sites in this zone" is unchecked, and then click the "add" button to the right of "add this website to this zone." Click Close.

3. Click the **Custom Level** button. First, change the "reset to" drop down box to "**Low**" and click **Reset**. You will receive a warning box asking, "Are you sure you want to change the settings for this zone?" Click **Yes**.

4. In the Security Settings selection, scroll down to each of the following and make the indicated changes:

a. Download unsigned ActiveX controls: change from Prompt to Enable

b. Initialize and script ActiveX control not marked as safe for scripting: change from Prompt to Enable

c. Allow web pages to use restricted protocols for active content: change from Prompt to Enable

d. Display mixed content: change from Prompt to Enable

e. Websites in less privileged web content zone can navigate into this zone: change from Prompt to Enable

f. Click OK. You will receive a warning box asking, "Are you sure you want to change the settings for this zone?" Click Yes. Click OK.

5. **Refresh the home page**

6. The Remote Control web page should be fairly straight forward; however, there are a few things to note:

a. You do **not** need to type in HSEN or NYS before the workstation name or the user name you are accessing.

b. When launching remote control, a user does not have to be logged in **unless** you are remote controlling a Windows 2000 machine.

c. If a user is logged on to a machine attempting to remote control, they will be prompted with a dialog box asking them if they want to grant remote control to the USER ID of the person attempting to remote control their machine.*

d. If no user is logged on, or if the machine is locked, Windows Remote Desktop will be launched (not available with Windows 2000).

e. The remote control tool for Windows 2000 is slightly different in appearance from the tool used with Windows XP.

***It is important to let the user know the User ID, so that while attempting to remote control their machine they can accept (or deny).

Questions

For local districts:

If you have any questions or concerns related to this Notification, please contact the Coordination Center at 1-800-603-0877 or send an email to: oft.sm.cns.coordination.center@oft.state.ny.us

For voluntary agencies:

Questions regarding this notification should be directed to either mailbox:
Internal: ocfs.sm.deployment
External: ocfs.sm.deployment@ocfs.state.ny.us

New York State Office of Cyber Security and Critical Infrastructure Coordination Information Bulletin

Subject: Malicious Email Messages Referencing a Postcard from Hallmark

Multiple states have reported an increase in email messages with the subject of "POSTCARD FROM HALLMARK". These malicious emails have included a zip file called "postcard.zip" although the malicious attachment and subject line will probably change to avoid detection. At this time, it is believed that the file contains malware which is a new variant of myDoom. Once the malware is run, it sends copies of itself to other internal users and random external hosts.

Analysis of the associated malware has shown connections to numerous hosts. These hosts include msdirect.servicemail24.de (84.17.190.211), mail.lebanon-online.com.lb (64.26.62.254), msdirectservices.com (193.189.224.91) and lebanon-online.com.lb (64.26.62.254). Other indications of infection are the presence of the file msmg.exe and the associated registry key HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run "" = C:\WINDOWS\system32\msmg.exe. Another report of similar findings can be found at http://www.threatexpert.com/report.aspx?md5=dec558ed05a4e33c7f71769d3832f107. Additional analysis indicates that the current domains to be sending the initial email are rsys1.com and responsys.net. However note that the originating email servers can change at anytime.

Due to the numerous variants of the malware, antivirus software is not always successful in identifying and quarantining the malware. Therefore, user education and awareness is of utmost importance in preventing the spread of this malicious email.

Additionally, one state has reported that the malicious host which sent out this greeting card was associated with source IP address 77.85.192.51(Executive Agency for Seed Control, Bulgaria). In this particular instance, after the user opened the card, their machine starts sending IRC traffic to 194.109.20.90 (XS4ALL).

Be advised that attackers may use the upcoming holiday season and other current events (such as the 2008 Presidential Election and Inauguration) to entice users to visit Web sites, click on links, open attachments, or perform other actions that could lead to system compromise.

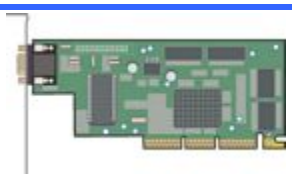
Recommendations:
We recommend considering the following actions:

- Consider blocking zip attachments at the email gateway.
- Do not open unexpected email attachments even from trusted sources.
- Ensure that all anti-virus software is up to date with the latest signatures.
- Ensure all critical system patches have been applied to the operating system and applications such as internet browsers.

NEW Postings to the CONNECTIONS Intranet

The following document(s) was recently posted to the CONNECTIONS intranet website:

- The CONNECTIONS NEWS
- Release Notes for Children Served with Missing Clinical Diagnosis Reports for LDSS and VA's



Weekly System Maintenance

Due to regularly scheduled system maintenance, the CONNECTIONS application will not be available on…

- Wednesday, 12/17/08 from 5:00 AM – 7:00 AM
- Friday, 12/19/08 from 5:00 AM – 7:00 AM

Office of
Children & Family
Services
Gladys Carrión, Esq.
Commissioner