

DSS ADMINISTRATIVE LETTER
PERFORMANCE MANAGEMENT/REPORTING AND EVALUATION MANAGEMENT
PM-REM-AL-06-10
DMA ADMINISTRATIVE LETTER NO: 05-10
DAAS ADMINISTRATIVE LETTER NO: 10-11

TO: County Directors of Social Services
County Security Officers

DATE: July 15, 2010

SUBJECT: Information Systems Security and the IRAAF

I. BACKGROUND

Version 3.0 of the Information Security Manual for the North Carolina Division of Social Services and County Departments of Social Services was issued July 1, 2009. The Information Resource Access Authorization Form (IRAAF) was also updated at that time.

Over the past several months, it has come to our attention that county security officers may be experiencing difficulties completing IRAAFs correctly. Errors on IRAAFs are contributing to a backlog at the DHHS Customer Support Center (CSC). In an effort to ease this backlog and to ensure access is granted and revoked timely, modifications to the IRAAF procedures will be implemented effective August 1, 2010. The purpose of this Administrative Letter is to outline these changes.

II. APPOINTMENT OF SECURITY OFFICERS

County Security Officers and backups must be appointed by the County DSS Director. The Security Officer Change Authorization Form (Appendix 5 in the Security Manual) must be completed and submitted to the Customer Support Center. CSC maintains a database of Security Officers.

III. RESPONSIBILITIES OF SECURITY OFFICERS

A. Security Officers and Backups

Security Officers are responsible for ensuring that the CSC has been provided the correct information regarding the current Security Officers and backups for their county. Updates must be submitted to CSC as soon as deletions/appointments are made. The Security Officer Change Authorization Form (Appendix 5) must be used for these updates. This form must be submitted to the Customer Support Center for processing. An email address must be listed on the form for the Security Officer and backup. It is recommended that counties review their Security Officers list at least every 6 months.

B. Appropriate Access

Security Officers are responsible for ensuring that appropriate access to State Information Systems is requested for all users via completion of the IRAAF. CSC is not responsible for identifying or correcting errors on the IRAAF where information is omitted or inappropriate access is requested. Therefore, time should be taken when requesting user access on the IRAAF to avoid having the IRAAF rejected, inappropriate access being given, and non-compliance with policies and regulations.

Appendix 11 of the Security Manual lists many of the DSS systems, the abbreviations used to identify the systems, and the staff who would be appropriate users of each. This Appendix should be used as a guide when requesting access.

Keep in mind that in accordance with Dear County Director Letter PM-REM-04-2007 (July 10, 2007), it is mandatory that an IRAAF be on file with DHHS Customer Support by August 31, 2010, for every employee with access to any State Information System.

C. ERIC Rights

DSS Security Officers may have ERIC rights. This must be noted on the Security Officer Change Authorization Form (Appendix 5). This access allows Security Officers to immediately revoke RACF access. This action must be taken by the Security Officer with ERIC rights while the IRAAF is in process to delete an individual's access. This will ensure that the individual will not have access to systems when access is no longer necessary.

D. Account Inactivity

After six months of inactivity, user access rights will be revoked by DHHS. This removes the RACF ID from the RACF table and all access associated with it. To avoid access being removed for employees who may be out for extended periods on disability or for other reasons, remind users to sign in using their RACF ID at least every 30 days. This will keep the RACF ID active and prevent it from being deleted from the table. In the event that a RACF ID is deleted and the individual continues to need the access, an IRAAF must be submitted to CSC.

More information is available in the Security Manual regarding Security Officers' responsibilities.

IV. CHANGES EFFECTIVE AUGUST 1, 2010

- A. IRAAFs submitted to CSC will no longer require Supervisor and Security Officer signatures (see item B below). However, IRAAFs will only be processed if emailed from a Security Officer on file with CSC. It is imperative that email addresses of Security Officers and backups be kept up-to-date. If an IRAAF is received and the email address does not match one on file, the form will be rejected.
- B. Although not required for submission to CSC, Security Officers and Supervisors must sign the IRAAF that is maintained in the county. **These signed forms must be retained in the county for audit purposes.**
- C. Security Officers will continue to be responsible for ensuring only appropriate access is requested and granted to users. IRAAFs must be completed correctly. If an error on the IRAAF results in inappropriate access, the Security Officer is responsible and must take the appropriate action to ensure the access is revoked immediately.

V. SECURITY REPORTS

RACF and OLV Monthly Access Control Reports, referenced in Dear County Director Letter, PM-REM-02-2010, AFS-03-2010, located at <http://www.dhhs.state.nc.us/dss/dcdl/perman.htm>, must be reviewed on a monthly basis. Security Officers must submit the required documentation as listed in this Dear County Letter to Performance Management Section by the 20th of each month.

Systems Security Reports, listed in the Security Manual, Section 3.3, Responsibilities, must be reviewed at least two times per year and documented on Appendix 13. This listing of reports will be updated in the next issuance of the Security Manual. The reports that must be reviewed include:

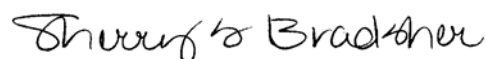
SYSTEM	REPORT NAME
County Administration Reimbursement System (CARS)	Cannot be reviewed at this time. Report under development.
Crisis Intervention Program (CIP)	In the CIP system, under the Reports Section, click on the County Staff Listing and select your county.
Central Registry	NCXPTR: DHRCYA CYA SECURITY REPORT
Client Services Data Warehouse (CSDW)	Cannot be reviewed at this time. Report under development.

SYSTEM	REPORT NAME
Eligibility Information System (EIS)	NCXPTR: DHREJA SECURITY REPORT BY COUNTY
Enterprise Program Integrity Control System (EPICS)	NCXPTR: DHRFRD FRD440-1 ACTIVE USERS
Employment Programs Information System (EPIS)	NCXPTR: DHRWFJ SECURITY-ACTIVE IDS
Foster Care and Adoptions	NCXPTR: DHRPQA SECURITY TABLE REPORT
Foster Care Facility Licensing System (FCFLS)	NCXPTR: DHRFCF FCF FCF900-1 SECURITY REP
Food Stamp Information System (FSIS)	NCXPTR: DHRSLA RACF SECURITY COUNTY RPT & DHRSLA RACF SECURITY REFERENCE (if needed)
Low Income Energy Assistance Program (LIEAP)	NCXPTR: DHREPA LIEAP SECURITY REPORT
SCCRS - SUBSIDIZED CHILD CARE (GH02)	NCXPTR: DHRGHB SCC STAFF SECURITY LIST
Services Information System (SIS)	NCXPTR: DHRSYA SYA SECURITY REPORT
SSRS – SMART START (GH02)	NCXPTR: DHRGHB SCC STAFF SECURITY LIST
TANF Data Collection System (TDC)	NCXPTR: DHRWRA TDC SECURITY RPT

As stated above, the Security Manual and the IRAAF will be updated/revised as soon as feasible. Our intent is to include county staff on a workgroup to make these changes to the manual and form. If you are interested in participating, please contact DSS Performance Management at 919-334-4530. In the meantime, should you have security questions, please contact us.

Systems security is very important to DHHS and our Divisions. We all must do our part to ensure only appropriate staff have access to North Carolina citizens' data.

Sincerely,



Sherry S. Bradsher

Craig L. Gray, MD, MBA, JD, Director
Division of Medical Assistance

PM-REM-06-2010

DMA ADMINISTRATIVE LETTER NO: 05-10

DAAS ADMINISTRATIVE LETTER NO: 10-11

Page 5

Dennis W. Streets, Director
Division of Aging and Adult Services

Deborah J. Cassidy, PhD, Director
Division of Child Development

SSB:HB:rr

cc: Lanier Cansler
Dan Stewart
Karen Tomczak
Pyreddy Reddy