DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE OF DIRECTOR

ACTION REFERRAL

TO	DATE
Supra	3-15-13

DIRECTOR'S USE ONLY	ACTION REQUESTED
1. LOG NUMBER 000287	[ ] Prepare reply for the Director's signature DATE DUE _____
2. DATE SIGNED BY DIRECTOR _____ cc: Mr. Keck, COS, Foot, Roberts ✓	[ ] Prepare reply for appropriate signature DATE DUE _____ [ ] FOIA DATE DUE _____ [X] Necessary Action

APPROVALS (Only when prepared for director's signature)	APPROVE	* DISAPPROVE (Note reason for disapproval and return to preparer.)	COMMENT
1.			
2.			
3.			
4.			

Brenda James

From: Jan Polatty
Sent: Friday, March 22, 2013 1:53 PM
To: Brenda James
Subject: FW: Audit Notification Letter: State of South Carolina's Medicaid Management Information System Security Controls (Report Number: A-04-13-05049)
Attachments: Audit Notification Letter_05049_ 03-12-13.pdf

Brenda, please make sure we logged this – I think I printed and gave to you..... thanks!

Please log this to Supra – copy TK, DS, Byron Roberts. (Copy not necessary to TK/DS as they have received electronically) Thanks, Jan.

From: Johnson, Brian C (OIG/OAS) [mailto:Brian.Johnson@oig.hhs.gov]
Sent: Wednesday, March 13, 2013 10:02 AM
To: Anthony Keck
Cc: John Supra; Jan Polatty; Mann, Cynthia (CMS/CMCS); Olin, Elaine M. (CMS/CMCS); Daly, Kay L (OIG/OAS); Pilcher, Lori S (OIG/OAS); Wilkinson, Tony D (OIG/OAS); Arman, Jeffrey J (OIG/OAS); Lehrer, Neil (OIG/OAS); Vallejo, Miguel (OIG/OAS); Zastrow, Chris P (OIG/OAS)
Subject: Audit Notification Letter: State of South Carolina's Medicaid Management Information System Security Controls (Report Number: A-04-13-05049)

Good Morning Mr. Keck,

Please see the attached audit notification letter informing you of our intention to audit the State of South Carolina's Medicaid Management Information System security controls (Report Number: A-04-13-05049).

Respectfully,

Brian C. Johnson
Manager, IT Audit / Advance Audit Techniques Staff
US Department of Health & Human Services
Office of the Inspector General
61 Forsyth St. SW, Suite 3T41
Atlanta, GA 30303
Ph: 404-562-7788 / Cell: 678-644-3299 / Fax: 404-562-7795

DEPARTMENT OF HEALTH AND HUMAN SERVICES

OFFICE OF INSPECTOR GENERAL

OFFICE OF AUDIT SERVICES, REGION IV
61 FORSYTH STREET, SW, SUITE 3T41
ATLANTA, GA 30303

March 12, 2013

Report Number: A-04-13-05049

Anthony Keck, Director
Department of Health & Human Services
1801 Main Street
Columbia, SC 29201

Dear Mr. Keck:

The purpose of this letter is to notify you of our intention to audit the State of South Carolina's Medicaid Management Information System (MMIS) Security Controls. The objective of our audit is to determine whether the State of South Carolina Department of Health & Human Services has implemented sufficient security controls over its MMIS.

The U.S. Department of Health and Human Services (HHS), Office of Inspector General (OIG) performs independent reviews of HHS programs pursuant to the Inspector General Act of 1978 (the Act). Section 6(a)(1) of the Act (5 U.S.C. App. § 6(a)(1)) authorizes OIG "... to have access to all records, reports, audits, reviews, documents, papers, recommendations, or other material available to HHS which relate to programs and operations with respect to which the Inspector General has responsibilities under this Act." Pursuant to 45 CFR § 92.42(e), HHS has the right of access to any books, documents, papers, or other records that are pertinent to the Federal grant to make audits, examinations, excerpts, and transcripts.

To expedite completion of our work, we request that you have the documents listed in the enclosure to this letter available at our entrance conference. During our review, we will also need access to additional documents and records. We appreciate your cooperation in this matter and will make every effort to minimize any disruption to the work of your office.

When transmitting any audit information to OIG over the Internet, please properly safeguard the information. We request that you use the HHS/OIG Delivery Server, not email or attachments to email. Information transmitted through the HHS/OIG Delivery Server complies with Federal Information Processing Standard (FIPS) 140-2, *Security Requirements for Cryptographic Module*. Please contact Brian C. Johnson, IT Audit Manager, at (404) 562-7788 or Miguel A. Vallejo, Senior Auditor, at (404) 562-7779 when you are ready to provide the requested information before our entrance conference. We will authorize your staff to use the HHS/OIG Delivery Server and give instructions in its use.

We are required to report as a security breach any audit information sent to us that does not meet FIPS 140-2 requirements.

This audit will be performed under the direction of Brian C. Johnson, Audit Manager. As arranged by Miguel Vallejo of his staff, we plan to hold an entrance conference on or about March 18, 2013. We request that you provide a work area for four auditors for approximately 1 month.

If you have any questions or concerns about our audit, please contact Brian C. Johnson, IT Audit Manager, at (404) 562-7788 or Miguel A. Vallejo, Senior Auditor, at (404) 562-7779 or through email at Brian.Johnson@oig.hhs.gov or Miguel.Vallejo@oig.hhs.gov, respectively. Please refer to report number A-04-13-05049 in all correspondence. Thank you for your attention to this matter.

Sincerely,

Lori S. Pilcher
Regional Inspector General
for Audit Services

Enclosure

cc:
Kay L. Daly, OIG OAS, AIG for Grants, Internal Activities, and Information Technology Audits
Tony Wilkinson, OIG OAS, IT Audit Director
Cindy Mann, Center for Medicaid and CHIP Services, Deputy Administrator and Director
Elaine Olin, Center for Medicaid and CHIP Services, Data & System Group Director

Initial Request List
(Please provide information in electronic format whenever possible. For requested lists, please provide as tables or text files.)

Please provide us with, or access to, the following requested items:

1. Narrative description and diagram of the Medicaid Management Information System (MMIS) network architecture including external connections.

2. Narrative description and diagram (flowchart) of the Medicaid claims process.

3. Organizational charts including names and titles and individual(s) responsible for system security for:

    1) Department of Health & Human Services,

    2) Information Security, and

    3) Network Administration.

4. Security plans for the MMIS, including the contractor's plans if applicable.

5. Reports and corresponding corrective action plans (as follows):

    1) two most recent SAS-70 reviews,

    2) two most recent risk analyses, and

    3) any other IT reports from the past 12 months.

6. For the most recently completed year:

    1) total number of Medicaid claims processed by DHS,

    2) total dollar value of claims processed, and

    3) total number of beneficiaries for whom claims were processed.

7. Policies and procedures for the following Information Technology areas:

    A. system backup and restore;
    B. encryption;
    C. use of anti-virus software for all computers and portable devices;
    D. patch management;
    E. firewalls;
    F. wireless access;

G. access controls including account authorization, establishment, modification, and security;
H. audit logging and/or audit controls;
I. passwords;
J. remote user access;
K. security awareness training;
L. inventory controls;
M. workstation security;
N. contingency plan;
O. security incidents;
P. vulnerability scanning;
Q. risk assessment;
R. media sanitization and disposal;
S. protection and movement of electronic protected health information; and
T. personnel:

a. hiring, transfers, and terminations;

b. security awareness training for new and existing employees; and

c. job rotation, vacation, initial background, and periodic reinvestigation requirements.

8. Inventory list of all servers to include:

A. server name;
B. operating system (e.g., Unix, Linux, Windows, Novell) and version;
C. primary function/service (e.g., DB, File, Domain Controller, Exchange, Web, Backup, email, print, DNS, Remote Access/VPN, and Application);
D. name of system manager; and
E. MAC addresses.

9. Inventory list of desktops, laptops, and mobile system devices to include:

A. device name;
B. device type (e.g., laptop, desktop, iPad, Macs, tablet, and cellular phone);
C. operating system and version;
D. primary function; and
E. MAC addresses.

10. List of network devices (e.g., routers, firewalls, switches) to include:

A. manufacturer and model number,
B. software version, and
C. primary function.

11. List of anti-virus scanning software to include:

    A. product name,
    B. version, and
    C. modules used for servers and workstations.

12. Anti-virus vendor contracts.

13. List of anti-virus scan exclusions including:

    A. file names,
    B. file extensions, and
    C. attachment names that are being filtered (outgoing and incoming).

14. Most recent 10 virus infection reports or system virus logs.

15. Patch management software documentation for systems, network devices, and portable devices to include:

    A. product name,
    B. version, and
    C. modules used.

16. Vulnerability scanning software documentation for systems, network devices, and portable devices to include:

    A. product name,
    B. version,
    C. platform supported, and
    D. "computer name" of the server where each of these tools resides.

17. Last two vulnerability scanning reports.

18. Central log/event analysis product documentation for servers and network devices to include:

    A. product name,
    B. version, and
    C. modules used.

19. Central log or event report showing correlated or critical events for the past 3 months.

20. List of active employees to include the following fields:

    A. user ID,
    B. first and last name,
    C. hire date, and

D. position.

21. List of terminated, retired, and transferred employees from January 1, 2012, thru present to include the following fields :

    A. user ID(s);
    B. first and last name;
    C. date of termination, retirement, or transfer; and
    D. position.

22. List of network user accounts to include the following fields:

    A. user ID,
    B. user name,
    C. user groups to which that employee belongs,
    D. creation date,
    E. password status,
    F. account status,
    G. last use/activity date, and
    H. last password change date.

23. List of service accounts to include the following fields:

    A. user ID,
    B. purpose,
    C. user name,
    D. system groups to which that service account belongs,
    E. creation date,
    F. password status,
    G. account status,
    H. last use/activity date, and
    I. last password change date.

24. List of high-level access users to include system, domain, network administrators and power users, detailing the following fields:

    A. user ID,
    B. user name,
    C. user groups to which that administrator belongs,
    D. creation date,
    E. password status,
    F. account status,
    G. last use/activity date, and
    H. last password change date.

25. List of remote user accounts (e.g., virtual private networks, etc.) to include the following fields:

    A. user ID,
    B. user name,
    C. user groups to which that employee belongs,
    D. creation date,
    E. password status, and
    F. account status.

26. Naming conventions for the Department of Health & Human Services and mainframe system software data sets, online transactions, and other items.

27. Contracts for third-party-supplied services (e.g., processing facilities, telecommunications, and storage facilities).

Mainframe Specific

28. List and organization chart identifying RACF and z/OS operators and administrators.

29. List of security administrators responsible for granting system and application access to Mainframe.

30. Report from most recent Internal and External penetration testing.

31. List of all individuals that have access to or promote changes to the production environment and their job title (e.g., coders, implementers).

32. Evidence of the latest review of user access violations.

33. Evidence of the last user access review/re-certification.

34. RACF installation policy, procedures, and system user manual.

35. Any reports concerning activity, e.g., other audit reports, special projects, studies, consolidation of user access into one RACF account per individual.

36. The name, title, role(s), and responsibilities of the individual(s) responsible for installing, monitoring, and maintaining RACF.

37. SETR LIST.

38. Listing of all:
    A. production applications,
    B. system support applications on Mainframe,
    C. load libraries,
    D. critical databases, and

E. data set names.

39. List of all users to include:
    A. user-id
    B. user ID,
    C. user name,
    D. user groups to which that employee belongs,
    E. creation date,
    F. account status,
    G. password status,
    H. last password change date,
    I. last use/activity date,
    J. role/responsibilities, and
    K. permissions.

40. List of all Group profiles and the Superior Group owner.

41. List of all resources not protected or fully protected by RACF.

42. Procedures outlining use of RVARY command.

43. Procedures/criteria for assigning "SPECIAL," "OPERATIONS," and "AUDITOR" attributes to users/groups.

44. Employee Confidentiality and Non-Disclosure policy.