



Audit Department

500 S Grand Central Pkwy Ste 5006 • PO Box 551120 • Las Vegas NV 89155-1120
(702) 455-3269 • Fax (702) 455-3893

Angela M. Darragh, CPA, CFE, CISA, Director

July 9, 2015

Mr. Don Burnette
Clark County Manager
500 South Grand Central Parkway, 6th Floor
Las Vegas, Nevada 89106

Dear Mr. Burnette:

We recently completed an audit of the Clark County Fire Department (CCFD) Sansio application. The audit was conducted in accordance with our annual audit plan and covers the period from May 1, 2014, to June 30, 2014. The last day of fieldwork was January 20, 2015. The objective of this audit was to determine whether application controls governing the Sansio system provide reasonable assurance of the confidentiality, integrity, availability of the CCFD's protected health information (PHI) in accordance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) requirements.

We found that controls to protect the integrity, confidentiality, and availability of PHI accessed through Sansio can be improved. We found areas that leave the data at risk, including the following:

- Limited ability to assess risk to CCFD PHI;
- Toughbook inventory location discrepancies;
- User access control, administration, and activity log issues;
- Inadequate disaster recovery and business continuity planning and testing; and
- Billing and accounts receivable/reconciliation issues.

A draft report was provided to the Clark County Fire Chief for comment, and his response is included.

We appreciate the cooperation and assistance provided by the staff of the Clark County Fire Department.

Sincerely,

Angela M. Darragh, CPA
Audit Director



AUDIT DEPARTMENT

Audit Report

Clark County Fire Department Sansio Application Audit

July 2015

Angela M. Darragh, CPA, CISA, CFE
Audit Director

AUDIT COMMITTEE:

Commissioner Steve Sisolak

Commissioner Chris Giunchigliani

Commissioner Lawrence Weekly

TABLE OF CONTENTS

BACKGROUND 1

OBJECTIVES, SCOPE, AND METHODOLOGY 2

RESULTS IN BRIEF 3

DETAILED RESULTS 3

Limited Ability to Assess Risk to CCFD’s PHI (HIGH) 3

Toughbook Inventory Locations Not Correct (HIGH) 5

Toughbook Hard Drives Not Encrypted (MEDIUM) 5

Inadequate User Administration (MEDIUM)..... 6

User Activity is Not Monitored (MEDIUM) 6

No Disaster Recovery or Business Continuity Plan (MEDIUM)..... 7

Collection and Write-Off Procedures for Aging Receivables Need to Be Established 7
 (MEDIUM) 7

Billing Delays and Errors (MEDIUM) 7

No Reconciliation of Revenue and Accounts (MEDIUM) 8

MANAGEMENT RESPONSE..... 9

BACKGROUND In 2010, the Clark County Fire Department (CCFD) contracted with Sansio, Inc. for the use of Sansio's HealthEMS application. This application provides a Software-as-a-Service (SaaS) solution to the CCFD. Sansio provides web-based access to software that the CCFD first-responders access using Toughbooks (ruggedized laptop computers) to record the medical information they collect during a response, and is subsequently used to bill for the first responders' services. Sansio provides all updates and support for the proper operation of the software application, and the CCFD's data is maintained at offsite data centers. The CCFD is responsible for managing the Toughbooks and users. The medical information that is recorded, maintained, and processed in this system is considered Protected Health Information (PHI) and is subject to special requirements for the proper safeguarding of the information because the CCFD is a covered entity under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

When emergency calls are received at the CCFD, the call number assigned by the computer-aided-dispatch (CAD) system populates an incident number in the HealthEMS application. Date and location data are populated as well. When first responders arrive on-scene and begin entering information, the application has built-in checks to ensure front end data completeness, accuracy, and integrity. The application also encrypts data as it is entered and transferred via the internet to offsite storage. Once transferred, the application automatically deletes data from the Toughbook. After all edit checks are cleared, the data is ready to be retrieved by Intermedix, the CCFD's billing and collection vendor. Intermedix retrieves incident information daily during weekdays. Intermedix prepares and sends out invoices to insurance companies and patients (as applicable). On a monthly basis, Intermedix provides CCFD with a billing, collection, and accounts receivable report.

The existing contract with Sansio expires in November 2015.

OBJECTIVES, SCOPE, AND METHODOLOGY

The objective of this audit is determine whether:

- Application controls governing the Sansio system provide reasonable assurance to the CCFD of the confidentiality, integrity, and availability of the CCFD's protected health information (PHI) in accordance with HIPAA requirements.

To accomplish our objective, we assessed system user and administrator access roles by comparing a HealthEMS system user matrix with employee information from SAP (the County's enterprise resource software) to determine whether employees with access were actively employed by the CCFD and whether access was appropriate based on employee positions. We also searched for duplicate and generic user accounts (IDs) and reviewed system password policy parameters. In addition, we assessed Sansio application controls, user access controls, and change management activity for existence, adequacy, and adherence.

We also conducted ride along emergency response observations to document the response process, the use of the Toughbook and the HealthEMS application, and the handling of protected health information.

Using incident activity information from May and June 2014, the following procedures were performed:

- We tested 10 Toughbook inventory items for existence and usefulness.
- We reviewed 14 incidents from an Intermedix monthly report and traced each incident to HealthEMS, recalculated each incident, compared each amount to an Intermedix invoice billed, and traced receipts collected to the bank statements and to SAP.
- We compared various response times for 13 incidences between information from HealthEMS, Intermedix, and Visinet.
- We compared patient transport numbers between information from CCFD, HealthEMS, and Intermedix for May and June 2014.

- We compared emergency response service rates between Intermedix and Clark County Business License for consistency.

Our review included an assessment of internal controls in the audited area. Any significant findings related to internal control are included in the detailed results. The last day of fieldwork was January 20, 2015.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

RESULTS IN BRIEF Our audit identified various system monitoring, inventory safeguarding, and information reporting processes which could be strengthened.

During our testing, we found:

- Limited ability to assess risk to CCFD PHI;
- Toughbook inventory locations incorrect;
- User access control, administration, and activity log issues;
- No disaster recovery or business continuity plan; and
- Billing and accounts receivable/reconciliation issues;

Each finding includes a ranking of risk based on the risk assessment that takes into consideration the circumstances of the current condition including compensating controls and the potential impact on reputation, customer confidence, safety and health, finances, productivity, and the possibility of fines or legal penalties.

DETAILED RESULTS

Limited Ability to Assess Risk to CCFD's PHI (HIGH) The CCFD is not able to fully assess risks to the confidentiality, integrity, and availability of the PHI that CCFD entrusts to Sansio. This is primarily due to the lack of contractual rights that the CCFD can use to gather data on security activities, operations, and their related operating effectiveness at Sansio. There is no audit clause in the

contract with Sansio, and there is no defined third-party security assessment requirement.

The contract does contain language that allows the CCFD and the Audit Department to gather copies of Sansio's policies relevant to significant components of Sansio's operations. However, the documents provided by Sansio were limited to policy statements on critical items such as: general HIPAA compliance, breach notifications, risk assessment and management, disaster recovery, and business continuity. No procedural or other documented detail was available to demonstrate compliance in these areas on a day-to-day basis. Sansio representatives did provide written assurances that Sansio complies with the policies and routinely conducts activities to ensure the confidentiality, integrity, and availability of client PHI.

Sansio also provided an opinion letter from a Public Accounting Firm which conducted Type II Statement on Standards for Attestation Engagements (SSAE) 16/Service Organization Controls (SOC) 1 and SOC 2 examinations on the data center that stores CCFD's PHI. An SOC 1 examination reviews an organization's internal controls over financial reporting, while an SOC 2 examination evaluates an organization's information system relevant to security, availability, processing, integrity, confidentiality and/or privacy. However, this assurance is limited to only the data center component of the system in place for administering the Sansio application. In addition, the firm that conducted the assessment recognizes that this type of assessment does not equate to an assessment for HIPAA security rule compliance. Therefore, this assessment cannot be relied upon as a complete assessment of risks to the CCFD's PHI.

While Sansio did provide documentation that provides insight into their security and risk assessment activities, as well as that of their data center, the CCFD's overall ability to assess the risk to the CCFD's PHI is ultimately limited. The CCFD is at risk for regulatory fines if it cannot demonstrate that it assessed risks to the PHI it entrusted to Sansio. In addition, the CCFD's patients are at risk for harm if their data is compromised because not all risks to their data were recognized and mitigated.

Recommendation

1. Include an audit clause in future contracts with external service providers.
2. Evaluate whether independent security assessments of the Sansio application should be required in order to better assess risks to the CCFD's PHI, and which assessment is acceptable.

Toughbook Inventory Locations Not Correct (HIGH)

The Fire Departments uses Toughbook equipment (laptops) to record emergency response activity. Each device costs about \$4,500. Emergency personnel use the HealthEMS application on the Toughbooks to record patient information, which includes (PHI).

We selected 5 Toughbooks from the inventory report to verify if the equipment was at the location noted in the report. We found 3 instances in which the Toughbook was found to be in a location different than what was listed on the report. We also selected 5 Toughbooks located in the field and compared them to the inventory report. We found that 3 of these 5 Toughbooks were not listed in the physical locations where we initially observed them.

Without accurate inventory records, Toughbooks could be lost or stolen without the ability to determine where the loss or theft occurred. Due to the confidentiality of information, it is important to keep track of the hardware so that breaches are identified and addressed in a timely manner.

Recommendation

1. Update and maintain the Toughbook inventory report on a monthly basis.
2. Perform an annual review of inventory to verify existence, location, proper accountability, and usefulness.

Toughbook Hard Drives Not Encrypted (MEDIUM)

The CCFD has not configured the Toughbooks to encrypt the device hard drive. Toughbooks are in use by first responders all over the Las Vegas Valley on a daily basis. To the extent that any sensitive or confidential information may be stored outside of the Sansio application, it cannot be considered secured if a Toughbook is lost or stolen, even if the Toughbook is password protected.

Recommendation

1. Configure Toughbooks to encrypt the device hard drive.

Inadequate User Administration (MEDIUM)

The CCFD does not have procedures in place to appropriately add, drop, or assign users' access to data based on their employment status or role in the department. As a result, we noted active users no longer employed with the CCFD and users with access levels that do not appear aligned with their job duties. Specifically, we found:

- 26 users with system administrator access that allows these users to access, edit, or delete any record or report.
- 7 Information Technology employees assigned to the "Battalion Chief" role which allows users to edit reports and productivity numbers.
- 3 duplicate accounts.
- 3 users that we could not locate at all in SAP employment records.

Without user administration procedures that operate effectively, the confidentiality and integrity of CCFD's PHI data is at risk.

Recommendation

1. Develop and implement procedures to appropriately add, drop, and assign user access to data based on employment status and role in the department.

User Activity is Not Monitored (MEDIUM)

The CCFD does not routinely monitor user access to records in the HealthEMS system, which is a procedure required under HIPAA in order to detect unauthorized access to records. System reports are available to conduct this monitoring, but the CCFD does not monitor user activity in the system. In addition, the CCFD user access control policy does not include user account lockout/re-establishment procedures.

Without user monitoring controls in place, the CCFD lacks the ability to prevent or detect unauthorized user activity. The confidentiality, integrity, and availability of CCFD's PHI data are at risk.

Recommendation

1. Develop and implement procedures to monitor user activity for inappropriate user behavior.

No Disaster Recovery or Business Continuity Plan (MEDIUM)

The CCFD does not have a business continuity or disaster recovery plan for the HealthEMS incident tracking and management system. HIPAA requires covered entities maintain disaster recovery and business continuity plans to ensure the availability of PHI in the event of a disaster or outage (45 CFR 164.308(a)(7)).

Violations of HIPAA standards can result in fines of up to \$1.5 million per standard not followed for every year the standard is not followed.

Recommendation

1. Collaborate with Sansio representatives and CCIT to establish a disaster recovery and a business continuity plan.

Collection and Write-Off Procedures for Aging Receivables Need to Be Established (MEDIUM)

We found that accounts receivable at the time of our fieldwork was over \$500,000, of which over \$400,000 was older than 90 days. There is no contractual obligation for Intermedix to pursue collection for accounts older than 90 days. In addition, the CCFD currently does not review accounts receivable balances for collectability or potential write-off, in accordance with Nevada Revised Statute (NRS) 354.255/6.

Without collection and write-off procedures in place, the CCFD is potentially losing revenue, cannot evaluate their revenue performance, and is not in compliance with NRS.

Recommendation

1. Develop and implement collection and write-off procedures for aging receivables, including whether to contract with Intermedix for these services.

Billing Delays and Errors (MEDIUM)

When billing to and collecting fees from insurance companies for emergency services provided, it is important to prepare and send out correct invoices in a timely manner to avoid charges from being stale-dated (denied by the payor due to a delay in receiving a bill) or denied due to regulatory and contractual non-compliance.

In reviewing 10 incident records, we found that 7 claims were billed within two weeks of the incident date, which we believe is an acceptable period. However, we noted 3 claims that were billed three months to a year after the date of service. We also found 1 incident was incorrectly billed using 2012-13 service rates rather than the 2013-14 rates, which were in effect at the time of service.

In reviewing the June 2014 Intermedix monthly report where the incorrect invoice was uncovered, we found an additional 6 claims that were also billed incorrectly using 2012-13 rates. Typically, any rate changes occur at the beginning of a calendar year. CCFD provides Intermedix with a new rate schedule by the end of January each year. These 7 claims were for service dates between March 2013 and January 2014, but were billed by Intermedix using 2012-13 rates.

Recommendation

1. Amend the contract to require Intermedix to submit invoices within 30 days of the date of service.
2. Develop self-monitoring procedures to verify that bills are developed using correct rates.

No Reconciliation of Revenue and Accounts (MEDIUM)

We reviewed fee collection information for May and June 2014 and found that there is no reconciliation of fees collected between information from Intermedix, SAP, and the bank statement. Monthly reconciliation procedures should be in place where ever fees are collected to ensure all revenue is properly collected and recorded. In this case, the process should include a review and reconciliation of fees recorded in SAP, on the bank statement, and from Intermedix.

Reconciliations are a standard internal control to prevent waste or fraud, and to ensure proper recording of revenue in financial accounts.

Recommendation

1. Develop and implement reconciliation procedures to ensure revenues are properly collected and recorded.



Fire Department

575 East Flamingo Road • Las Vegas NV 89119
(702) 455-7311 • Fax (702) 734-6111



Greg Cassell, Fire Chief
Erik Newman, Sr. Deputy Fire Chief
Kelly Blackmon, Deputy Fire Chief • Jon Klassen, Deputy Fire Chief
John Steinbeck, Deputy Fire Chief • Roy Session, Deputy Fire Chief • Jeff Buchanan, Deputy Fire Chief
"Responding with Integrity – Serving with Compassion"



MEMORANDUM

TO: Angela M. Darragh, Audit Director
FROM: Greg Cassell, Fire Chief 
SUBJECT: Physio-Data Solutions (Sansio) Audit
DATE: June 29, 2015

The following information is the Clark County Fire Department (CCFD) management response to recommendations received after completion of the Physio-Data Solutions (Sansio) Electronic Patient Care Record system audit completed by your department from December 1, 2014 - May 1, 2015.

CCFD has used the Sansio E-PCR system since 2010. From inception to present time, CCFD field personnel have completed over 600,000 patient care reports. These reports are used to document all treatment provided to the patients who access 911 for medical issues or trauma related injury, and are completed in near real time. Because of the robust system that Sansio has developed, CCFD senior management is able to mine data entered in these reports to assess delivery of care, response times and patterns, and other quality assurance metrics. The Sansio system provides all documentation in an electronic format which enables CCFD to remain HIPAA compliant and make adjustments quickly and efficiently as HIPAA regulations change and evolve. The system as a whole enables CCFD to document, monitor, and adjust strategies to provide optimal care to those we serve.

We recognize the effort that went into the audit by your staff to understand a complex and vital system in our department and appreciate the insight provided to allow us to strengthen and improve upon an already robust and useful system. These recommendations were made by your department followed by our response.

RECOMMENDATION # 1: (HIGH)

CCFD has a limited ability to fully assess risks to the confidentiality, integrity, and availability of PHI that CCFD entrusts to Physio-Data Solutions (Sansio). We recommend that an audit clause be included in the next contract to evaluate whether independent security assessments should be required to better assess risks to CCFD PHI.

BOARD OF COUNTY COMMISSIONERS
STEVE SISOLAK, Chairman • LARRY BROWN, Vice Chairman
SUSAN BRAGER • TOM COLLINS • CHRIS GIUNCHIGLIANI • MARY BETH SCOW • LAWRENCE WEEKLY
DONALD G. BURNETTE, County Manager

MANAGEMENT RESPONSE:

Requested documents have been provided by Physio-Data Solutions (Sansio) to the Internal Audit Department to determine if adequate risk assessments are available from Physio-Data Solutions (Sansio). CCFD is waiting to hear back from Internal Audit to ensure that the internal procedures followed by Physio-Data Solutions (Sansio) minimize the potential risk to CCFD PHI (protected health information). The contract with Physio-Data Solutions (Sansio) expires in November, 2015. CCFD will work with Clark County Purchasing to ensure that recommendations from Internal Audit are included in the new contract. Documentation of third party security assessments when performed will be included to ensure continued HIPAA compliance in the future.

RECOMMENDATION #2: (HIGH)

We recommend that CCFD maintains a monthly inventory report on all mobile hardware used to create patient care records. An annual inventory report should also be completed to verify existence of, location, and usefulness of all mobile hardware.

MANAGEMENT RESPONSE:

CCFD will develop a more detailed policy/procedure in cooperation with internal IT staff to complete random asset verification on 10 units per month. Documentation on the exchange of damaged or non-functioning tablets will also be included in the policy/procedure to ensure accurate inventory location. CCFD will perform an annual review of inventory during the annual SNHD EMS inspections and in compliance with Clark County's Annual Asset Inventory due June 30th each year.

RECOMMENDATION #3: (MEDIUM)

We recommend that all mobile hardware hard drives be encrypted.

MANAGEMENT RESPONSE:

Purchase and deployment of new mobile hardware is anticipated to occur during the third quarter of 2015. The addition of Bitlocker technology to each new hard drive will fulfill this requirement.

RECOMMENDATION #4: (MEDIUM)

We recommend that CCFD improve and develop procedures to appropriately add, drop, and assign user access to data, based on employment status and specific role of the individual in the department.

MANAGEMENT RESPONSE:

CCFD will update and enforce the policy and procedure for Physio-Data Solutions (Sansio) user accounts. This will ensure that changes to or additions of user accounts are updated as user roles change.

RECOMMENDATION #5: (MEDIUM)

We recommend that CCFD develop and implement procedures to monitor all user activity for inappropriate behavior.

MANAGEMENT RESPONSE:

CCFD will develop and monitor a weekly report which will show access to the Physio-Data Solutions (Sansio) software system by individual user. An internal policy will be developed to ensure compliance with HIPAA regulations in regards to Physio-Data Solutions (Sansio) account lockout and re-establishment procedures.

RECOMMENDATION #6: (MEDIUM)

We recommend that CCFD collaborate with Physio-Data Solutions (Sansio) and CCIT representatives to establish a disaster recovery and business continuity plan.

MANAGEMENT RESPONSE:

Physio-Data Solutions (Sansio) has provided copies of their Disaster Recovery Plan to CCFD. This plan has been provided to Internal Audit to ensure compliance with Clark County policy. CCFD will develop a policy to allow for the use of a hard copy Patient Care Record in the event that electronic data becomes unavailable for an extended period of time.

RECOMMENDATION #7: (MEDIUM)

We recommend that CCFD develop and implement improved collection and write off procedures for aging receivables to include whether to contract with private billing vendor for these services.

MANAGEMENT RESPONSE:

Clark County follows the required method of collection outlined in NRS and has developed a write off policy. CCFD will utilize this policy and work with the Clark County DA office to fully implement the policy over the next 6 months.

RECOMMENDATION #8: (MEDIUM)

We recommend that CCFD amend the contract with Intermedix to submit invoices within 30 days of date of service. Intermedix and CCFD will develop self-monitoring procedures to verify that bills are developed using correct rates.

MANAGEMENT RESPONSE:

Intermedix will conduct a monthly review of accounts without a patient invoice, date of service, or claim file date to determine why the invoice/claim has not been mailed. Incorrect address, return mail, and missing insurance billing information are all reasons for delays in billing. Intermedix will regularly review the chargemaster in the billing system to ensure that the correct rates are being used for billing.

RECOMMENDATION #9: (MEDIUM)

We recommend that CCFD, in cooperation with Intermedix, develop and implement improved reconciliation procedures to ensure that revenues are properly collected and recorded.

MANAGEMENT RESPONSE:

CCFD will develop and implement reconciliation procedures to ensure revenues are properly collected and recorded within 90-120 days. Intermedix will perform monthly reconciliation between Physio-Data Solutions (Sansio) billable transports and accounts in Intermedix to ensure all billable trips are entered into Intermedix. Intermedix will reconcile the bank statement monthly with Intermedix End of Month Reports to ensure payments are recorded in Intermedix. Intermedix will reconcile the monthly bank statement deposits to the monthly Intermedix invoice to ensure the fees are correct.