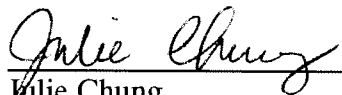


**UNIVERSITY OF CALIFORNIA, IRVINE  
ADMINISTRATIVE AND BUSINESS SERVICES  
INTERNAL AUDIT SERVICES**


**NEW HOSPITAL SECURITY AUDIT  
Report No. 2010-206**

**December 22, 2010**


Prepared by:

  
\_\_\_\_\_  
Julie Chung  
Senior Auditor

Reviewed by:

  
\_\_\_\_\_  
Gregory Moore  
Health Sciences Audit Manager

Reviewed by:

  
\_\_\_\_\_  
Bent Nielsen  
Director

December 22, 2010

**FRED LAUZIER  
ANCILLARY SERVICES SENIOR DIRECTOR**

**RE: New Hospital Security  
Report No. 2010-206**

Internal Audit Services has completed the review of the New Hospital Security and the final report is attached.

Please let us know if we can provide any additional support or assistance.



Bent Nielsen  
Director  
UC Irvine Internal Audit Services

Attachment

C: Terry Belmont  
Alice Issai  
Scott Martin  
Patricia Thatcher  
Audit Committee

**NEW HOSPITAL SECURITY**  
**Report No. 2010-206**

**I. EXECUTIVE SUMMARY**

In accordance with the Fiscal Year 2009-2010 audit plan, Internal Audit Services (IAS) reviewed the adequacy of the internal controls surrounding the processes for granting, maintaining, and monitoring controlled door access under the C•CURE system for the University of California, Irvine Medical Center. Based on the audit work performed, some of the C•CURE internal controls need to be strengthened to ensure compliance with University policies and procedures. Specifically, we noted the following observations:

- **Employee, and temporary badge process and procedures** – The internal controls surrounding the issuance, monitoring, collection, storage, and disposal of employee and temporary badges needs improvement. The observations related to these processes are Department Procedures for Badges (Observation A), Inconsistency in Documentation, Notification, and Guidelines Requirements (Observation B), Collection, Storage, and Disposal of Badges (Observation C), and Card Numbers and Temporary Badges. (Observation D);
- **C•CURE database maintenance** – The internal controls over the process of granting or disabling secured door access needs improvement. In addition, the review found individuals linked to two, three, and/or four sets of badge data within the C•CURE database. (Observation E);
- **Leaves of absence** - Currently there is not a process or practice in place to notify Security to disable badges when employees start their leave of absence. In addition, a process has not been established to collect the badges of employees who are out on leave. (Observation F);
- **C•CURE Monitoring** – This observation relates to real time monitoring of door access control, closed-circuit television (CCTV) cameras, digital video recorders (DVR) as well as third party devices such as fire alarms, intercoms, burglar and other alarms. (Observation G).

These issues are discussed in detail below.

**II. BACKGROUND**

IAS conducted an audit of the new hospital security system, C•CURE 8000. In September 2008, C•CURE was installed in UC Irvine Douglas Hospital and implemented in December 2008. With this system, the Security department is able to control and monitor door access rights issued to UC Irvine Medical Center staff and affiliates. For C•CURE access purposes only, staff include faculty, staff, residents, and medical and nursing students. Affiliates are non-payroll personnel such as

**NEW HOSPITAL SECURITY**  
**Report No. 2010-206**

School of Medicine sponsored groups (non-UCI physicians, interns, and students) and other contracted service providers (registry, Bio-Medical Engineering, and vendors).

With the gradual implementation of C•CURE 9000 in late May 2010, the risks of unauthorized access to some medical center buildings resulting in theft, property damage, and personal injury will be further minimized through secured door access and monitoring.

**III. PURPOSE AND OBJECTIVES**

The purpose of the audit was to evaluate the adequacy of the internal controls surrounding the processes for granting, maintaining, and monitoring controlled door access under the C•CURE system.

The objectives of this review were as follows:

1. Determine if policies and procedures have been established and implemented for the badge issuance, replacement, and collection process;
2. Determine if the controls over the badge issuance and replacement process are adequate to ensure only authorized employees, vendors, and consultants have been issued a badge;
3. Determine if the processes for granting controlled door access and maintaining the C•CURE database are adequate to ensure only authorized personnel have access as defined in the C•CURE system;
4. Determine if departmental controls over temporary badges have been established and are functioning as intended;
5. Determine if the current monitoring processes and controls in place are adequate to determine if it is effective and efficient, and ensures security;
6. Determine if the C•CURE hardware is located in a secured area and that physical access and privileges to the C•CURE system is limited to authorized personnel.

**IV. CONCLUSION**

In general, processes and the administration of the C•CURE system appear to be functioning as intended. Two departments, Human Resources (HR) and Security, work together to provide and ensure appropriate door access rights. However,

**NEW HOSPITAL SECURITY**  
**Report No. 2010-206**

business risks and control concerns were identified in control procedures for badges, C•CURE database maintenance, leaves of absence, and C•CURE monitoring.

Observation details and recommendations were discussed with management, who formulated action plans to address the findings. These details are presented below.

**V. OBSERVATIONS AND MANAGEMENT ACTION PLANS**

**A. Department Procedures for Badges**

**Background**

Security has the responsibility for issuing specialty badges to departments who then distribute them to medical center affiliates defined as non-payroll personnel. Once departments receive these badges from Security for door access use, they have the responsibility of controlling badge issuance and use.

**Observation**

IAS reviewed six medical center departments' business practices in maintaining a total of twelve sets of badges. Four of the departments received one set of badges, one department received two sets of badges, and the last department received six sets of badges. It should be noted that seven sets of badges (five for one department and one each for two departments) were designated for use during one business day or shift only.

**1. Inventory Maintenance and Review**

A detailed review of the badge inventory process disclosed that three of the six departments did not review the logs, and perform an inventory of the badges on a daily basis. The following is a summary of the IAS badge inventory review:

a. In one department four sets of temporary badges were designated for use during one shift or 12 hours. IAS found that a total of 68 of 175 (39%) badges were unaccounted for and considered missing. A detailed summary of the review is as follows:

1. Twenty two of 65 (34%) badges programmed with access to medication rooms that were set aside for contractor use were not listed as issued that morning and were considered missing;

**NEW HOSPITAL SECURITY**  
**Report No. 2010-206**

2. Twenty one of 50 (42%) badges programmed with basic door access that were set aside for contractor use were not listed as issued for use that morning and were considered missing;
  3. Twenty one of 30 (70%) badges with access to medication rooms that were set aside for staff use were not listed as issued for use that morning and were considered missing; and
  4. Four of 30 (13%) badges with basic door access that were set aside for staff use were not listed as issued for use that morning and were considered as missing.
- b. Three of 21 badges for another department were identified as missing. Department personnel were not able to determine when these badges became missing;
  - c. Personnel for another department were unaware that one of its seven badges was lost, until it was found and returned to the department five days later.
2. Insufficient Documentation, Badge User Identity, and Enforcement

IAS reviewed department records used to document badges issued for use. The review disclosed that the records were insufficient and incomplete to ensure an adequate control environment for all six departments. The following issues were noted:

- a. Two departments did not ensure individuals that were issued badges had a valid or legitimate reason to access doors in the medical center including access to medication rooms;
- b. Six departments did not identify, verify and document each individual that was issued a badge for four of the eight sets of badges reviewed;
- c. One department required individuals to leave their driver's license as insurance to return the key ring and badge. However, the department returned the driver's license although the key ring was returned without the badge attached.

In all cases Security was not initially notified of the missing badges.

Inventory control procedures should be developed and implemented to ensure temporary badges are accounted for daily and by the end of each shift. Missing badges should be reported to Security at the time of discovery. In addition, the

**NEW HOSPITAL SECURITY**  
**Report No. 2010-206**

departments should have controls in place to ensure adequate follow up to deactivate badges if appropriate. Also, the departments should have procedures in place to properly collect, destroy, and document badges that are no longer being used due to issuing replacement badges, separation, or termination.

**Management Action Plan**

Policies and procedures are being developed for the ID badge program along with the revision of the ID badge guidelines. The estimated target date is June 2011.

A departmental badge sign in/out sheet has been developed and is being sent to all departments that were issued specialty badges for their use.

Departmental audits of specialty badges have been initiated by the Security Systems Coordinator and will continue on an on-going basis approximately every four months for each department.

**B. Inconsistency in Documentation, Notification, and Guidelines Requirements**

**Observation**

A review of the badge replacement process disclosed that requirements as stated in the guidelines are not always followed or enforced. Specifically, we noted the following:

1. There was not a process or practice in place where Security was notified of lost or stolen badges and the date a badge is lost or stolen is not documented. In addition, when a new badge is created and issued, data for the issued badge is transmitted to Security. However, the reason for issuing the badge was not included. Consequently, Security did not know if a badge was issued to replace a worn, damaged, lost, or stolen badge or if it was issued to a new employee;
2. A written management request is not always obtained prior to replacing worn or damaged badges. Department staff stated that it has been their business practice to only visually note that a badge is worn or damaged before issuing a new badge;
3. The replacement fee is not always collected when replacing a lost badge. Department personnel indicated that this practice is not strictly adhered to, but is discretionary.

**NEW HOSPITAL SECURITY**  
**Report No. 2010-206**

**Management Action Plan**

These issues will be addressed with the roll-out of the new badge database. This system, managed by the Sr. Analyst Security Systems Coordinator working in the Security department, will allow Security to document lost or stolen badges, replacements, and actions that are being taken. Since July of 2010 a system to charge a replacement fee has been implemented for anyone who has lost a Vendor, Hospital or Contractor Access Badge. A replacement fee is also charged for any other UC Affiliate or Contract Employee who is not on payroll. The plan is for all badge processing to be handled by Security by March 2011.

In some cases, exceptions have been made for collecting payment for a lost badge, e.g. the Emeritus professor who has worked for the University for more than 50 years was not charged for the loss of his badge. Our new badge policy will more clearly specify when the fee will be collected for lost badges, and in what types of situations exceptions may be made.

**C. Collection, Storage and Disposal of Badges**

**Observation**

Our review disclosed that controls are not in place to ensure proper collection, storage, and disposal of badges that are worn, damaged, and unused or are no longer used due to separation or termination. Records of when and which badges were collected and disposed of were not maintained. The business practice was to store unused badges in open plastic containers that are placed on the counter in the HR reception area. In addition, a small supply of new, blank badges were not securely stored, but kept in the reception area on the counter and easily accessible to other employees as well as non-employees.

Control procedures should be implemented to ensure the proper collection, storage, and disposal of badges and to prevent unauthorized use of the badges collected. In addition, new, blank badge working stock should be securely stored to reduce the risk of theft or misappropriation.

**Management Action Plan**

With the oversight of badges moving from HR to Security and the implementation of the new online ID Badge Request System, authorized requestors will be prompted to select a radial button within the badge request that notifies the Badge Administrator that the employee's ID Badge has been surrendered and collected by the requestor. The Security Systems Coordinator has implemented a badge destruction log. All ID badges that are retrieved from employees are listed on the destruction log by name and proxima card number. In addition, all proxima cards



**NEW HOSPITAL SECURITY**  
**Report No. 2010-206**

that are used in the creation of badges that have errors or are misprints are also listed in this destruction log. At regular intervals ID badges that are collected are shredded to ensure that no badges or information can be used. In addition, all badge making materials located in the Security Department are kept under lock and key and are not accessible to other employees or the public.

**D. Card Numbers and Temporary Badges**

**Background**

Door access readers "read" the unique five digit badge card number on the back of each badge to grant appropriate door access as programmed in the C•CURE database.

A temporary badge is issued when the newly hired employee information update has not yet been completed in the API system. In addition, there are times where an individual starts working at the medical center as either a contractor, volunteer, or student, and is later hired as a medical center employee.

**Observation**

IAS reviewed badges issued and programmed with door access rights and noted the following:

1. There were no records documenting the card numbers for ten badges issued to Facilities contractors. In addition, five of the ten card numbers had already been issued to five QUEST consultants in the prior month. As a result, the C•CURE database provided the Facilities contractors with the same door access rights as the QUEST consultants;
2. Security was not notified to disable temporary badges in C•CURE once a replacement badge with an employee identification number (EIN) has been issued and the badge data has been transmitted for import to C•CURE. As a result, there were two sets of badge data, one with a badge card number and another with an EIN, in C•CURE linked to one individual. However, only one badge data is current and valid.

Control measures over issued badge card numbers and temporary badges should be developed to ensure that a unique badge card number is only linked to one badge and individual. In addition, notification of temporary numbers should be sent to Security in order to maintain current valid data and disable the old, invalid data in C•CURE.

**NEW HOSPITAL SECURITY**  
**Report No. 2010-206**

**Management Action Plan**

Since July 2010, Security maintains an ID badge sign out log. Pre-printed numbered proxima cards come in batches of 50 cards, 200 to a box. When a new batch of 50 cards is ready for use the cards are inventoried and the numbers are checked to make sure no duplicate numbers have been printed by the manufacture. An ID badge sign out log is created for those 50 cards in number sequence. When a badge is made the information for that badge including name, date and signature of recipient is documented on that log. If a printing error is made for that ID card, it is noted on the ID badge sign out log for that unique proxima number and a new badge is printed. On occasion the Time ID system indicates that a proxima number is already in use. When this occurs, the blank proxima card is removed from the machine and this is noted on the ID badge sign out log.

Since the primary responsibility of creating ID badges has moved to the Security Department and we now have access to the Time ID badge making system we can now run a name search and verify how many ID badges have been issued to a particular person with a particular name. The personnel creating the badge can now ask the new badge recipient about previous badges issued and those badges can be deactivated even though they have not been turned in.

**E. C•CURE Database Maintenance**

**Observation**

IAS reviewed the C•CURE database report dated April 12, 2010 to determine if the data was accurately maintained in C•CURE. Test work was performed to determine if door access was granted or disabled in a timely manner and if appropriate badge information was entered in C•CURE. The following is a summary of the findings:

1. The supporting documentation was reviewed for 18 staff members that separated or were terminated from February 28, 2010 through March 6, 2010 and the following was noted:
  - a. Eight of 18 (44%) badges were disabled more than one month after the employees' last day of work;
  - b. Five of 18 (33%) badges were not deactivated as of April 12, 2010;
  - c. Three of 18 (17%) badges reviewed were not found in the C•CURE database;

**NEW HOSPITAL SECURITY**  
**Report No. 2010-206**

- d. Stop notices were sent to Security for 11 of the 18 (61%) employees sampled between one and 16 days after they separated or were terminated from the medical center.

The notification process should be reviewed and training provided as needed to ensure badge access rights are disabled in a timely manner in order to prevent unauthorized door access.

IAS also found individuals linked to two, three, or four sets of badge data within the C•CURE database. As a result, a "clean-up" of the C•CURE database is necessary in order to identify and disable the badge data that is no longer current and valid to ensure the database is accurate.

**Management Action Plan**

This process is now automated and terminated employees that are included in the API terminated employee report have their badges deactivated automatically at midnight on the date of termination.

**F. Leaves of Absence**

**Background**

Employees sometimes choose to take leaves which range from maternity/paternity leave, family medical leave (FMLA), military leave, and medical leave. Other employees are placed on administrative leave without pay and are barred from performing their regular duties.

**Observation**

Currently there is not a process or practice in place to notify Security to disable badges when employees start their leave of absence. In addition, a process has not been established to collect the badges of employees who are out on leave.

A review of the process disclosed an employee in the respiratory department was first terminated, later reinstated, and then placed on administrative leave. However, Security was only notified of the initial termination. A policy and procedure should be developed to notify Security in order to disable badges of staff on leave in a timely manner to ensure door access is secured.

**NEW HOSPITAL SECURITY**  
**Report No. 2010-206**

**Management Action Plan**

The University badge process will address this issue, as we will need to develop a process for informing all parties of HR actions that may take place. Procedures will be developed to ensure badges are disabled and collected for employees placed on investigatory leave. In addition, the disabling and/or badge collection process will be handled on a case by case basis for employees on leave of absence other than a leave arising from a disciplinary process.

**G. C•CURE Monitoring**

**Background**

In addition to door access control, the C•CURE system provides integration with critical business applications which includes, but is not limited to, the following: closed-circuit television (CCTV) cameras, digital video recorders (DVR) as well as third party devices such as fire alarms, intercoms, burglar and other alarms. Various locations inside and outside of four buildings are monitored in real time with 53 active CCTV cameras linked to four DVRs. Furthermore, reports available in C•CURE are also valuable monitoring tools.

**Observation**

IAS observations of current practices disclosed the following concerns.

1. Additional measures should be considered to increase effectiveness and efficiency in CCTV/DVR monitoring, as follows:
  - a. CCTV/DVR monitoring is limited to approximately 20% of the Security Systems Coordinator's time. Her time is divided among other duties which includes the following: maintaining the C•CURE database, issuing vendor and departmental badges, generating C•CURE reports for investigations, assigning user rights to the C•CURE system and resetting passwords, maintaining 17 doors that have been preset to be unlocked during regularly scheduled business hours, as well as other security duties. Therefore, monitoring may not be at an optimal level from a security standpoint;
  - b. Currently, two DVRs linked to 20 CCTV cameras located in one of four buildings are not interfaced with the C•CURE security system. Video feeds from these cameras are monitored on a separate network system. Therefore, monitoring may not be at an optimal level from a security standpoint.

**NEW HOSPITAL SECURITY**  
**Report No. 2010-206**

2. As an additional monitoring tool, there are several C•CURE reports that should be considered for the Security Systems Coordinator to review in order to identify and minimize possible building security issues.
  - a. The Security Systems Coordinator could run and review a C•CURE report on specific doors in high risk buildings that have been identified as being held or propped open repeatedly;
  - b. The Security Systems Coordinator could run and review a C•CURE report on badge inactivity to identify badges that have not been used in recent months for additional follow up including badge collection and deactivation.

**Management Action Plan**

An external consulting company is currently performing a security assessment of the hospital and security operations. Development and implementation of a Security monitoring center for twenty four hours a day coverage including monitoring CCTV and alarm systems will be based on the recommendation provided in the final report.