University of Michigan
University Audits

University Safety and Security Communication, Reporting and Incident Investigation

Issue Date: February 10, 2012

Distribution:
University of Michigan Board of Regents
M.S. Coleman, President
O.H. Pescovitz, Executive Vice President for Medical Affairs
T.P. Slottow, Executive Vice President and Chief Financial Officer
S. Scarnecchia, Vice President and General Counsel
E.R. Harper, Vice President for Student Affairs
S.J. Churchill, Vice President and Secretary of the University
D.L. Strong, Chief Executive Officer, UMHHC
T.A. Denton, Chief Operating Officer, UMHHC
D.C. Campbell, Chief Medical Officer, UMHHC
T.V. Peterson, Associate Hospital Director, Operations and Support Services, UMHHC
H.D. Baier, Associate Vice President for Facilities and Operations
L.J. Rullman, Associate Vice President for Student Affairs

2012-809

Safety and security touches all facets of University life and involves multiple stakeholders, from students, parents, staff, patients, and families to security and law enforcement agencies. Focused efforts on safety and security are a regular part of all aspects of campus and Health System operations. These efforts require substantial coordination and collaboration across many departments within the University.

On December 3, 2011, at the request of President Coleman, University Audits began conducting:

- A review of the internal controls breakdown that contributed to a delay in a thorough investigation of a case of suspected possession of child pornography by a medical resident at the hospital
- A comprehensive review of the internal control structure and environment related to safety and security at the University of Michigan-Ann Arbor campus

Both sections of the review involve the processes and people that conduct and manage the safety and security of the University's students, employees, and patients. The results of the reviews are discussed in this report:

- Section I – the breakdown of internal controls specific to the delay in reporting of a case of potential possession of child pornography in the hospital by a medical resident
- Section II – what must happen so that future potential criminal activity is managed in a seamless, collaborative way and the outcomes are timely, thorough, and transparent
- Section III – management's response to this report
- Addendum I – May 2011 and November 2011-to-date timeline of events related to the specific issue discussed in Section I
- Addendum II – Text of attorney client privilege communication

Section I

University Audits was asked to examine the internal controls related to an issue that was first reported in May 2011 but not fully investigated until November 2011. The case was closed in May because of a lack of evidence. When it was brought forward again in November, the case was fully investigated and additional evidence showed suspected wrongdoing on the part of a University of Michigan medical resident. (Please see attached Addendum I for a timeline of related events.)

Factors that caused the case to be stalled after the first attempt at investigation:

- Primary evidence that was viewed on a USB thumb drive attached to a hospital computer disappeared between the time it was first seen and the next morning.
- There was not a clear line of responsibility for investigating the case. The Office of the General Counsel inappropriately took ownership. Hospitals and Health Centers Security and Entrance Services (HHC-Security) and MCIT (Medical Center Information Technology) assisted in the investigation under attorney client privilege. The text of the attorney client privilege communication is attached as Addendum II.
- The lead attorney investigating the case made the determination that there was not enough evidence to file a police report and discontinued the investigation. The attorney is no longer employed with the University.
- HHC-Security did not log the case in the system shared with the Department of Public Safety (University Police-DPS). If that had been done, DPS would have seen that there was a potential issue.
- MCIT reviewed the computer internal logs where the USB thumb drive had been seen and was able to determine who had accessed the computer. MCIT was not able to retrieve other relevant information such as files accessed from a USB thumb drive.
- There was significant confusion about the roles of HHC-Security and DPS. Hospital employees who reported the incident thought they were talking to police when they were talking with HHC-Security. DPS is an accredited law enforcement agency with authority and responsibility to investigate, search, arrest, and use necessary force to protect persons and property. HHC-Security is responsible for providing security patrols and escorts, access control, visitor screening, way finding, and security camera/alarm monitoring.

DPS and HHC-Security have policies and procedures for their individual departments, but no specific guidance or communication protocols between their departments. If the following internal controls had been in place in May 2011, the delay in performing a thorough investigation may have been avoided:

- Shared documented responsibilities for all parties who have a need to respond: DPS, HHC-Security, Office of the General Counsel, Health System Compliance Office, and Office of Clinical Affairs.
- The Office of the General Counsel should be available for legal advice but should not take ownership of an investigation.
- Consistent logging of all potential criminal activity in a system that is shared by both HHC-Security and DPS.
- Clear, shared procedure that states when a case is reported by HHC-Security to DPS. The procedure should define shared and independent roles after the case is reported.
- Referring all computer forensic needs related to suspected criminal activity to DPS. DPS has trained information technology officers as well as sophisticated tools to examine technology evidence. MCIT should continue to assist in routine internal investigations related to HIPAA (protected patient health information) and other privacy breaches.

- Clear, simple information for anyone who may be reporting a security incident. This should include a process for giving feedback to the person who reports an incident to provide closure.

It is extremely important that management address the weak internal controls, as stated above, that relate to a specific set of circumstances. However, without a consistent approach, a culture of collaboration, and shared goals that deal with all types of criminal activity, the risks and control breakdowns we see in this specific case might cause a potentially more serious reporting and investigation outcome in the future. Section II of this report addresses the broader issue of all cases of potential criminal activity that require shared responsibility among departments within the Health System, HHC-Security, and DPS.

Section II

University Audits reviewed University communication and reporting processes related to security and potential criminal activity on the Ann Arbor campus to gain an understanding of the interdepartmental relationships and communication protocols related to public safety and security. The Flint and Dearborn campuses were not part of the review. The review included:

- Examining and assessing existing documentation of policies and procedures
- Interviewing senior management and other key personnel

The purpose of this report is advisory and is not intended to provide audit assurance. It is meant to provide a context and recommendations for leadership to consider for enhancing University safety and security communication and reporting processes on the Ann Arbor campus.

For the purposes of this report, the major safety and security units at the University of Michigan-Ann Arbor Campus include, but are not limited to the following:

Law Enforcement

Department of Public Safety (DPS) is a full service law enforcement agency with the authority and responsibility to investigate, search, arrest, and use necessary reasonable force to protect persons and property. DPS is responsible for enforcing the laws of the State of Michigan and the Ordinance of the Regents of the University of Michigan. DPS reports to the University Associate Vice President for Facilities and Operations.

Security Departments

University of Michigan Hospitals and Health Centers Security and Entrance Services (HHC-Security) is a separate security agency of the University and reports to the Hospital Associate Director for Operations and Support Services. HHC-Security provides security patrols and escorts, access control, visitor screening, way-finding, and security camera/alarm monitoring. Another primary role is to support patients, families, and visitors who are sometimes facing very difficult and traumatic challenges in their lives.

Housing Security is a unit of University Housing, within the Division of Student Affairs and reports to the Associate Director for University Housing. Housing Security is responsible for security, access control, and fire safety in University Housing owned and controlled properties. DPS receives and dispatches all housing security incidents.

Other Organizations that have a role in University Safety and Security

Office of General Counsel (OGC) is under the direction of the Board of Regents and the President. The Vice President and General Counsel conducts the legal affairs of and provides legal advice and representation for the University.

Office of Clinical Affairs is responsible for maintaining and improving the environment of patient care at the U-M Health System. It is also accountable for the quality of professional services by all individuals with clinical privileges within the Health System. The office reports to the Chief Executive Officer of U-M Hospitals and Health System and works closely with Risk Management, HHC-Security, and the Office of General Counsel to ensure patient care quality and safety.

Health System Risk Management is part of the Office of Clinical Affairs and is dedicated to minimizing the adverse effects of loss due to unforeseen events or situations that could result in harm to patients, staff, and visitors.

Risk Management Services assists the operating units and staff of the University to protect against or mitigate losses to the people, facilities, and other assets of the campus community. Risk Management reports to the Treasurer's Office.

The Health System Compliance Office promotes compliance with all laws/regulations governing billing, coding, Medicare and Medicaid, patient privacy, information security, vendor relationships, conflict of interest, and governmental investigations. The department's purpose is to maximize compliance with laws and regulations to minimize risk of violations and penalties. This office collaborates with *University Audits* in investigating and responding to calls to the University's confidential hotline.

Office of Emergency Preparedness provides resources, guidance, and training for the University community in matters related to emergency preparedness, response, and recovery. The Office of Emergency Preparedness reports to the Associate Vice President for Facilities and Operations.

Occupational Safety and Environmental Health (OSEH) provides monitoring, guidance, and education to promote health, safety, protection of the environment, and ensure compliance with local, state, and federal laws dealing with hazardous materials, operations, fire and life safety, and environmental protection. OSEH reports to the University Associate Vice President for Facilities and Operations.

Each of University of Michigan's safety and security organizations plays an essential role in providing our community with a safe environment. Cooperation and better communication between these units will make this essential mission more efficient and effective.

University Audits Observations and Recommendations

Communication Among University Safety and Security Organizations

University safety and security organizations have well established policies and procedures for day-to-day operations within their respective units. However, there are no formal protocols or memoranda of understanding between safety and security organizations for the shared responsibility of reporting suspected criminal activity or other security incidents.

Current safety and security policies need simplification and alignment among organizations. There needs to be common definitions and well understood escalation procedures for suspected criminal activity.

Recommendation: **Develop an extensive set of common guidelines and protocols for reporting security incidents throughout the University.** The protocols need to be actionable and should establish clear communication and procedures for hand-off of cases between University safety and security organizations. These practices can be in the form of checklists, online training, decision trees, and formal policies and procedures.

Communication protocols should include roles and responsibilities for all parties who need to react appropriately to a specific aspect of the case. Examples include:

- DPS, HHC-Security, and Housing Security when there is suspected criminal activity
- University Risk Management when there is loss of property
- Office of the General Counsel for legal analysis
- The Health System Compliance Office in cases where health related regulations may have been breached
- University Audits when internal controls may have been missing or bypassed
- Office of Clinical Affairs when a patient or health professional is potentially involved
- OSEH for occupational safety or environmental issues

Definitions of incident types are not well understood. Develop a comprehensive list of incident types. This should include definition of *potential* criminal activity as well as *proven* activity. Without a common definition of reportable activity, the course of investigation and ultimate resolution is seen differently and is one of the causes of disagreement and tension between departments.

Privacy and Law Enforcement

Concerns about student and patient privacy sometime impede timely communication of security and safety incidents to police and security agencies. In current practice, University employees are instructed to confer with the Health System Compliance Office and the Office of General Counsel if there are privacy concerns. Generally, records that contain protected health information or protected student records are not turned over to law enforcement without a subpoena. While privacy protection is a compelling, competing interest, both HIPAA and FERPA do allow disclosure of protected information to law enforcement in certain instances.

Recommendation: **Raise awareness of the different patient, employee, and student privacy rules.** Law enforcement and security officers should receive regular HIPAA and FERPA training to raise awareness and sensitivity to privacy. Commonly understood definitions are needed for when and under what circumstances protected information should be shared with security and law enforcement agencies. A streamlined process is needed when there is suspected criminal activity to ensure relevant protected information is shared with law enforcement through means that are legally appropriate.

Duty to Report

The University is subject to various legal requirements to report potential criminal activity and it is also subject to laws that restrict what information may be shared. These legal requirements can appear to be in conflict and may cause confusion about whether or not a report should be made. For example, laws that require reporting of certain crimes might conflict with laws that protect student, victim, or patient privacy.

Recommendation: **Foster better understanding and sensitivity of duty to report requirements.** Develop legal guidance and training to help responders navigate the complexities and grey areas of reporting suspected criminal activity.

Emergency Response

When an individual dials 911 from a University phone, including residence halls, the call goes directly to DPS for triage and dispatch. An exception exists within the hospital, 911 calls go directly to HHC-Security for triage and dispatch. This allows HHC-Security and medical providers to respond to medical emergencies and other non-emergent situations within the hospital. However, the routing of

911 calls to HHC-Security rather than DPS can cause confusion on the part of the reporting individual, who believes they are making a report to law enforcement.

> ***Recommendation:*** **Review the use of 911 triage and dispatch.** DPS and HHC-Security should have formalized dispatch procedures for the operation of each facility control center. Security officer responders should clearly identify themselves as security and not law enforcement.

Shared Reporting Systems

As of January 2012, DPS has implemented a new information management system that is not part of the internally developed system previously shared with HHC-Security and Housing Security. This system, CLEMIS (Courts and Law Enforcement Management Information System), is a multi-faceted, regional law enforcement management information system that allows sharing of data between nearly 100 Michigan law enforcement agencies. Because HHC-Security and Housing Security are separate from DPS and are not law enforcement, they will not have direct access to the new system, but will continue to need access to relevant incident reporting information within CLEMIS. Other security incident reporting and calls for service, such as lost and found, alarms, personal injury, and/or safety/hazard reports are tracked via separate reporting systems maintained by each of the Security Offices.

> ***Recommendation:*** DPS, HHC-Security, and Housing Security management have recently met to discuss the impact of CLEMIS on information sharing and to develop a work-around process to restore HHC-Security and Housing Security access to previously available safety and security information. **Create a shared communication system that facilitates accountability and cooperation.** Both HHC-Security and Housing Security need to be aware of crimes that have occurred in nearby areas of their responsibilities. Shared reporting mechanisms should be seamless, designed to share University-wide safety and security information, and facilitate communication protocols and decision processes.

Lessons Learned

One of the reasons that differing opinions exist about the outcomes of security incidents and criminal investigations is because there is not a consistent process to discuss the issues that arise between agencies or groups as they work toward a final resolution of each case.

> ***Recommendation:*** **Formally debrief on major security incidents.** Develop a process that gathers all groups involved in a case to discuss what worked well and what could have been done better. Learn from the experience so that positive actions are reinforced and the things that did not work to the satisfaction of everyone involved are discussed and resolved so that the process will be improved the next time there is a similar incident.

Training

Policies, procedures, and protocols are essential in defining a common understanding and providing a common roadmap for action in all types of cases. Additionally, to institutionalize a consistent approach to many different types of incidents and responses, it is important that everyone that may be involved in investigation and resolution of a case receive hands-on training related to these policies, procedures, and protocols. As an example, DPS will benefit by learning the reasons for protected health information safeguards as well as the reasons when it is essential to share protected information quickly and safely in a potential criminal case.

Recommendation: **Develop ongoing team-building training programs.** Develop a comprehensive training program that builds knowledge and understanding of processes from all perspectives, and builds a collaborative team effort for addressing many types of issues. Training can assist all parties understand the reasons for perspectives and regulations that impact the prescribed protocols, actions, and philosophies of others involved in a particular chain of response. Training should encompass the viewpoints of all parties and be attended by a cross-section of safety and security organizations.

Organizational Structures

Safety and security organizations at U-M report through multiple channels. There is no common reporting structure or mechanism. This is particularly problematic when it comes to police and security services. Each police/security agency reports to a separate organization and has separate and sometimes conflicting policies.

Recommendation:

- **Review the reporting lines and communication structure of police and security units.** Benchmark with other universities to provide examples of effective safety and security models. Consider the optimal structure given the complexities of our University for ensuring public safety and security.
- **Consider a DPS liaison office within the Health System.** There is no consistent DPS presence within the Health System. DPS officers are only interacting with hospital faculty and staff when there is a criminal investigation or an emergent situation. This contributes to tense working relationships and miscommunication.
- **Develop cross-functional teams.** Safety and security teams should be defined by incident type, and will ensure that the right skill sets are matched to respond to the particular issue. Teams should meet regularly in non-crisis mode to further develop understanding and trust.

Culture

A common understanding and single vision is needed among the University safety and security organizations. Competing and sometimes conflicting interests and a lack of role clarity have led to mistrust and suboptimal working relationships. There is a lack of understanding and appreciation for the contributions each organization makes to ensure a safe and secure work, learning, and patient care environment.

Recommendation: **The culture must change**. Define a plan to enhance team culture. Engage an outside expert to work with the leaders of the various security units and related areas to examine cultural issues that limit achievement of the common goals of the various units. This could be accomplished through a series of facilitated offsite meetings that bring the various parties together with a single vision. Without a cultural shift, there will continue to be breakdowns in the effectiveness of the organization as a whole.

Once there is willingness to come together with common goals and understanding, the points discussed in this report should be considered by all groups and individuals involved. Not all of these recommendations may be implemented as stated, but all should be part of the consideration in finding a working relationship that supports the best safety and security of all stakeholders at the University of Michigan.

Section III

Management's Response to Report

Incident Overview

On May 24, 2011, a medical resident initiated a report of one potential child pornography image based on review of three images on a USB thumb drive attached to a computer in a lounge for medical residents in the hospital. The initiation of the report included contact with faculty physicians for assistance and a request for direction from the Health System Compliance Office. The Health System Compliance Office referred the concern to Hospitals and Health Centers' Security Services and the Health System Legal Office on May 25, 2011.

Attorneys in the Health System Legal Office investigated whether there was evidence of criminal activity that should be reported to law enforcement. The lead attorney, a recent hire, had significant experience investigating and prosecuting health care professionals. She asserted control of the investigation, sought the acquisition of evidence from the computer in question, and interviewed the resident who reported that she may have seen evidence of child pornography. The lead attorney determined that there was not enough evidence to take the report to police and reported her conclusion to the Health System Legal Office, the Health System Compliance Office, and to the reporting resident. She closed her investigation in the first week of June 2011 and left the University soon thereafter for reasons unrelated to this incident.

At the time, those who were aware of the concern and investigation deferred to the lead attorney because of her expertise and assertion of control over the review, with the (mistaken) belief that the investigation was proper. In November 2011, the matter was raised again by concerned physicians in the wake of the Penn State incident, this time with the Office of Clinical Affairs, the department charged with ensuring every physician's competence to deliver safe patient care. Upon a second review, sufficient evidence was discovered that led to the termination and arrest of a suspect in the case.

Upon learning of the gap in reporting, President Coleman immediately ordered a review of the incident by University Audits to determine reasons and root causes for delayed reporting.

As a result of that review, it has been determined that the initial investigation was insufficient and improper:

1. The resident who reported the crime described the lead attorney who interviewed her as intimidating and threatening, causing distress and a feeling that she should not have come forward with the report.

2. The lead attorney's assertion of control over the investigation caused others in the Health System to cease their investigatory efforts, awaiting direction from Health System Legal Office.

3. The review of the computer by Health System personnel was insufficient and would have been enhanced if law enforcement had been involved to lead the investigation.

Beyond the role played by the attorney who is no longer with the University, management is concerned with the missed opportunity to appropriately report by others who were aware of the allegations in May, including:

1. The failure to report the potential crime to DPS and, instead, the decision to engage in an investigation through the legal office;

2. The decision to rely on the opinion of one attorney about the sufficiency of the evidence to determine whether or not a report would be made to DPS; and

3. The failure to recognize that in light of the possible risk to patient safety a report should be filed with the Office of Clinical Affairs or the Health System Risk Management Office to explore what protections might need to be put in place, even in the absence of a criminal investigation.

University management accepts responsibility for the delay in reporting the crime, an unacceptable handling of the reporting and necessary investigation of the concern regarding child pornography. We conclude that the assertion of improper control of the investigation by the attorney and reliance on her conclusions by others were the root cause for the delay and improper handling of the initial report. The case should have been forwarded to the Department of Public Safety in May.

Individual corrective action will be taken with the involved current employees to ensure greater clarity of their respective roles and the importance of vigilance when handling complaints of possible criminal activity or risk to patient safety. This corrective action will be documented in the employees' personnel files and those employees will be held accountable for improvement through the established performance review process.

To help determine how the specific circumstances arose that led others to rely on the conclusions of the lead attorney in this case, University Audits reviewed the particulars of this matter, as well as the overall status of safety and security operations at the University. During the course of review by University Audits, a number of observations were made involving the identification, reporting and handling of security and criminal investigations across the organization.

University management acknowledges the history of difficulties between DPS and Hospitals and Health Centers Security (HHC-Security). We accept the findings by University Audits that tensions between the two organizations contributed to the failure to report allegations of child pornography in May. We are determined to resolve these differences and create a positive safety and security culture across campus.

University Audits made a number of important recommendations to address the specifics of the incident in question as well as the systematic problems that contributed to it. Management accepts the recommendations and is committed to pursue the recommendations with strengthened policies, procedures, and training to prevent future lapses in protecting the safety and security of the patients we serve and the entire campus community.

Though not involved in this incident in any way, we believe it is important that Housing Security participate in our comprehensive efforts to ensure the development and implementation of a shared security vision campus-wide. The recommendations outlined below, therefore include Housing Security.

Specifically, Health System and Central Campus managers and staff will work together to develop an integrated response, reflecting the collaboration and interactions required to implement positive and sustainable changes in policies, practices, orientation, training, and culture. Some of the recommendations outlined in the audit report and this management plan are established or works in progress. Other recommendations will be pursued for timely implementation as summarized below.

Recommendation: **Develop an extensive set of common guidelines and protocols for reporting security incidents throughout the University.** The protocols need to be actionable and should establish clear communication and procedures for hand-off of cases between University safety and security organizations. These practices can be in the form of checklists, online training, decision trees, and formal policies and procedures.

> **Management Response:** Leadership in the following departments and offices will work collaboratively to develop recommendations for common guidelines regarding suspected criminal activity: Office of General Counsel, Health System Compliance Office, Health System Risk Management, Hospitals and Health Centers Security (HHC-Security), Housing Security, DPS, and others as appropriate.
>
> It will be made clear that, pursuant to these guidelines, suspected criminal activity is to be reported to the Department of Public Safety for investigation. An action plan consisting of draft policies, procedures, and other material with timelines needed to implement this recommendation will be written within 90 days**.**

Recommendation: **Raise awareness of the patient, employee, and student privacy rules.** Law enforcement and security officers should receive regular HIPAA and FERPA training to raise awareness and sensitivity to privacy. Commonly understood definitions are needed for when and under what circumstances protected information should be shared with security and law enforcement agencies. A streamlined process is needed when there is suspected criminal activity to ensure relevant protected information is shared with law enforcement through means that are legally appropriate.

> **Management Response:** It is essential that all safety and security personnel have broad understanding of the laws that govern access to student and patient records. While we have no doubt that there are key staff members in all of our safety and security offices with deep understanding of HIPAA and FERPA, we are committed to broadening this knowledge. The Office of the General Counsel has the lead to develop the training plan, with support from HHC-Security, Housing Security, DPS, Human Resources, and the Health System Compliance Office. The plan will be developed, including a schedule for implementation within 90 days.

Recommendation: **Foster better understanding and sensitivity of duty to report requirements.** Develop legal guidance and training to help responders navigate the complexities and grey areas of reporting suspected criminal activity.

> **Management Response:** Management will issue a memo to deans, department heads, and directors as a reminder of the importance and obligation of the duty to report suspected criminal activity in accordance with relevant law. This memo will be issued by February 20, 2012.
>
> We will prepare a plan to provide all safety and security personnel a working understanding of the potential conflicts in the "duty to report" requirements and privacy requirements under various laws, such as those governing health care, education, victim and whistleblower protection, and the Clery Act and how those sometimes conflicting requirements should be balanced in the health care and campus environment.

A specific training program will be developed by OGC with support from Human Resources, within 90 days, with training to be initiated no later than 120 days. Refresher training will be offered on an annual basis.

Recommendation: **Review the use of 911 triage and dispatch.** DPS and HHC-Security should have formalized dispatch procedures for the operation of the facility control center. Security officer responders should clearly identify themselves as security and not law enforcement.

Management Response: Health System and Central Campus leadership are committed to review 911 public safety answering points (PSAP) requirements and standard operating procedures to ensure the response to every 911 call is held to the highest standards of effectiveness, coordination, and efficiency. This review will be initiated by March 1, 2012.

Recommendations: **Create a shared communication system that facilitates accountability and cooperation.** Both HHC-Security and Housing Security need to be aware of crimes that have occurred in nearby areas of their responsibilities. Shared reporting mechanisms should be seamless, designed to share University-wide safety and security information, and facilitate communication protocols and decision processes.

Management Response: DPS, HHC-Security, and Housing Security management recently met to discuss the impact of CLEMIS on information sharing and to develop a process for HHC-Security and Housing Security to access safety and security information that meets criminal justice information requirements. Both HHC-Security and Housing Security need to be aware of crimes that have occurred in nearby areas of their responsibilities. Shared reporting mechanisms should be seamless and designed to share University-wide safety and security information, and facilitate communication protocols and decision processes.

The first phase of providing access to the DPS Security Center was implemented on February 3, 2012.

Recommendation: **Formally debrief on major security incidents.** Develop a process that gathers all groups involved in a case to discuss what worked well and what could have been done better. Learn from the experience so that positive actions are reinforced and the things that did not work to the satisfaction of everyone involved are discussed and resolved so that the process will be improved the next time there is a similar incident.

Management Response: Existing debrief processes are currently utilized in the University, including in the U-M Office of Emergency Planning and at the Health System through its Office of Clinical Affairs, following significant or “adverse” events.

These processes will be utilized on a more routine basis after major security incidents occur, to ensure an opportunity for “lessons learned” sessions. Part of this process will be to determine what worked well and to identify opportunities for improvement in a problem-solving and non-blaming atmosphere. Immediately, these sessions will occur after major security incidents and, in the future, the sessions will be based on procedures developed as a result of this management response.

Recommendation: **Develop ongoing team-building training programs.** Develop a comprehensive training program that builds knowledge and understanding of process from all perspectives, and builds a collaborative team effort for addressing many types of issues. Training can assist all parties understand the reasons for perspectives and regulations that impact the prescribed protocols, actions, and philosophies of others involved in a particular chain of response. Training should encompass the viewpoints of all parties and be attended by a cross-section of safety and security organizations.

> **Management Response:** We are committed to develop an active training program to ensure knowledge and understanding as central to a team-building effort between and across all safety and security units. This training will be integrated with other training efforts described earlier, developed in consultation with the Office of the General Counsel, Health System Compliance Office, Human Resources, DPS, HHC-Security, Housing Security and other units as necessary. This training program will be developed within 90 days and initiated within 120 days. The leadership of the security units will be responsible to provide orientation and refresher team training on a regular basis (at least twice per year).

Recommendations:

- **Review the reporting lines and communication structure of police and security units.** Benchmark with other universities to provide examples of effective safety and security models. Consider the optimal structure given the complexities of our University for ensuring public safety and security.
- **Consider a DPS liaison office within the Health System.** There is no consistent DPS presence within the hospital. DPS officers are only interacting with hospital faculty and staff when there is a criminal investigation or an emergent situation. This contributes to tense working relationships and miscommunication.
- **Develop cross-functional teams.** Safety and security teams should be defined by incident type, and will ensure that the right skill sets are matched to respond to the particular issue. Teams should meet regularly in non-crisis mode to further develop understanding and trust.

> **Management Response:** We are committed to exploring best practices and to determine if alternative approaches might yield benefit to the University. We will benchmark against peer institutions to review police and security reporting lines and organizational structures, with a benchmarking report completed within six months.
>
> Regarding the liaison idea, we will expand options to enhance visibility of DPS officers in the patient care environment, including routine orientation, training, and unit visits. Our goals include improved communication, collaboration, and outreach. We will include the liaison office or officer concept among the options available to meet these goals.
>
> The leaders of HHC-Security and DPS will provide an action plan to enhance ongoing DPS presence within 90 days.

Recommendation: **The culture must change.** Define a plan to enhance team culture. Engage an outside expert to work with the leaders of the various security units and related areas to examine cultural issues that limit achievement of the common goals of the various units. This could be accomplished through a series of facilitated offsite meetings that bring the various parties together with a single vision. Without a cultural shift there will continue to be breakdowns in the effectiveness of the organization as a whole.

Management Response: We believe that creating a culture of mutual respect and understanding is essential to creating a safe and welcoming environment for all. We will develop an approach to measure the culture and identify ways to enable an improved sense of collaboration and teamwork between and across our safety and security units.

Management accepts the recommendation to bring in external expertise for a full assessment of the working relationship and operational issues with HHC-Security, DPS, and the units with whom they interact regularly, in order to address significant cultural and management issues that have arisen in the course of this internal review.

The University's Associate Vice President for Human Resources, the Health System's Chief Human Resources Officer, and the Associate Vice President for Student Affairs have accepted lead roles to retain one or more outside experts who will assess our safety and security culture and help us achieve needed change. The outside expert(s) will be brought on board by April 1, 2012 and an implementation plan and schedule will be developed within the following 60 days.

Ora Pescovitz

Ora H. Pescovitz, M.D.
Vice President for Medical Affairs

Timothy P. Slottow
Vice President and Chief Financial Officer

Suellyn Scarnecchia

Suellyn Scarnecchia
Vice President and General Counsel

Report Conclusion
Everyone that we interviewed was dedicated to providing safety and security for the people, places, and things in their sphere of responsibility. Because there is limited sharing of information or collaboration in planning and execution of incident response, there is significant difference in approach and outcome. Without an in-depth, facilitated culture shift, policies, procedures, and protocols will not be universally understood and accepted or have long-term viability.

University Audits will conduct quarterly follow-up reviews until all noted risks are appropriately mitigated. These reviews will begin June 2012.

Carol F. Senneff

Carol F. Senneff
Executive Director University Audits

Sherry Cogswell

Sherry Cogswell
Senior Audit Manager University Audits

:

Addendum I

Chronology of Events

The chronology is based on interviews the Office of University Audits conducted. Dates and events are outlined according to the best recollections of those interviewed.

5/23/11 - Monday

- Late in the evening, a female pediatric resident (Female Resident) discovers a USB thumb drive left in a computer in a medical residents' lounge. In an attempt to identify the owner so that she can return the drive, she opens files on the USB thumb drive and sees the name of a male medicine-pediatric resident (Male Resident) on a document in one of the files. Another file contains a picture of adult pornography; a third contains a photo that she believes may be child pornography. She panics, closes the files, and leaves the residents' lounge, leaving the USB thumb drive. She goes home for the night.

5/24/11 - Tuesday

- The Female Resident returns to work in the morning and goes back to the residents' lounge to retrieve the USB thumb drive, but it is gone.
- The Female Resident reports what she saw to the Attending Physician on the same service. The Attending Physician consults with the Chair of the Medical School Department Compliance Officers (Compliance Chair).

5/25/11 - Wednesday

- The Compliance Chair contacts the Health System Chief Compliance Officer (Chief Compliance Officer). The Chief Compliance Officer arranges for the Compliance Chair to make a report to the Office of General Counsel (Health System Legal Office), and Hospitals and Health Centers Security and Entrance Services (HHC-Security).
- The Compliance Chair speaks with an attorney from the Health System Legal Office and an HHC-Security Supervisor, and relates the Female Resident's allegations.
- Within the Health System Legal Office, the attorney assigned to medical staff affairs assumes the lead role in the case (Lead Attorney). The attorney who took the original report continues to assist the Lead Attorney throughout the Health System Legal Office investigation (Assisting Attorney).
- The Attending Physician and the Compliance Chair arrange for the Female Resident to meet with HHC-Security. The Female Resident recounts the information described above (5/23) to the HHC-Security Supervisor and an HHC-Security Officer.
- After the meeting, the Female Resident and the HHC-Security officers go to the residents' lounge to look at the computer in question.
- The HHC-Security Supervisor contacts a Data Security Analyst in MCIT (Medical Center Information Technology) and requests assistance in analyzing what information can be gathered from the computer hard drive.
- The HHC-Security Supervisor leaves a voicemail for a Department of Public Safety (DPS) Police Sergeant asking whether DPS could provide some forensic assistance with images viewed on a computer from a USB thumb drive. (The phone message to DPS was never returned.).
- The Assisting Attorney sends an e-mail to the Data Security Analyst and the HHC-Security Supervisor. They are advised that their work is confidential and under attorney client privilege. The text of the e-mail can be found in Addendum II.
- The attorneys follow up with a confirming call to the HHC-Security Supervisor.

- The HHC-Security Supervisor told University Audits he did not complete a report to the police because of the e-mail (Addendum II) from the Health System Legal Office that he believed meant he should stop.
- The Data Security Analyst begins providing the attorneys with the May 23/24, 2011 computer records that confirm that the Male Resident in question logged into the computer before and after the reporting Female Resident. There were no other intervening log-ins during that time frame.

5/26/11 - Thursday

- The Health System Legal Office requests a meeting with the Female Resident. Due to scheduling conflicts, the meeting is set for 5/31, and then rescheduled to 6/2.

6/2/11 - Thursday

- The Lead Attorney interviews the Female Resident; the Assisting Attorney could not be there due to scheduling conflicts. The Female Resident leaves the interview crying.
- The Lead Attorney tells the Assisting Attorney that the Female Resident was unsure of her story and what she saw.

On or about 6/2/11

- The attorneys call the Health System Chief Compliance Officer and relay that there is not sufficient evidence to move forward, that the Health System Legal Office's assessment was that the Female Resident's story was shaky.
- The Lead Attorney reports to the Associate Vice President and Deputy General Counsel (Health System Affairs) that there was no evidence and that the case would be closed.
- The Female Resident texts the Attending Physician to tell her the meeting did not go well. She says the attorney told her the investigation is complete and the claims are unfounded. There was no evidence of child pornography on the computer. The Attending Physician tells the Female Resident she wants to follow up with the attorney, but the Female Resident asks her not to.

6/9/11 - Thursday

- The last day of employment of the Lead Attorney. The attorney's departure is unrelated to the case.

11/11/11 - Friday evening

- One of the original reporting physicians (Attending Physician) contacts (via phone call) the Risk Management Top Executive who is part of the Office of Clinical Affairs in the Health System. Two recent events caused the Attending Physician to come forward to raise questions about the case:
    - She learned that the attorney who had investigated the case in May (Lead Attorney) had left the University.
    - The Penn State incident occurred.
- The Attending Physician expressed concern about the treatment of the Female Resident and the outcome of the May case. The Risk Management Top Executive tells her this is the first time he had heard of the allegations.

11/12/11 - Saturday

- The Risk Management Top Executive meets with the Female Resident who originally found the USB thumb drive.
- The Risk Management Top Executive briefs the Chief Medical Officer for the Health System about the Attending Physician's phone call and the meeting with the Female Resident.

11/14/11 - Monday

- The Risk Management Top Executive contacts the Deputy General Counsel (Health System Affairs) and shares the Female Resident's account of the May incident and the Health System Legal Office meeting.
- The Chief Medical Officer confers with Chair of the Department of Pediatrics and Communicable Diseases (Pediatric Chair), and confirms that the Male Resident will be carefully supervised until appropriate action including precautionary suspension under the Medical Staff Bylaws can take place.
- Efforts were made to schedule a meeting with the Female Resident. It took several days to bring everyone together.

11/17/11 - Thursday

- The Chief Medical Officer, the Director of Pediatric Education, and a Health System Legal Office attorney meet with the Female Resident. She speaks in detail about what she saw on the drive, and they find her account convincing.

11/18/11 - Friday

- The Office of Clinical Affairs and Health System Legal Office make a report to HHC-Security, with the understanding that they will immediately make a report to the Department of Public Safety (University Police-DPS).
- HHC-Security reports allegations to DPS.
- DPS advises the Office of Clinical Affairs and Health System Legal Office that they will send a detective to begin investigation but then determine that no detective was available until Monday, 11/21/2011.

11/21/11 - 12/02/11

- DPS conducts investigation: interviewing numerous witnesses, obtaining forensic evidence, and reviewing the case with the Prosecuting Attorney (11/21 – 12/16).
- Clinical Affairs and others aware of the allegations are asked by DPS not to contact the Male Resident or tell others. They are told not to remove him from service as it would alert him and evidence could be destroyed.
- The Chief Medical Officer reviews the Male Resident's files, and notes no performance issues or patient complaints. The Chief Medical Officer and department leadership continue active monitoring of the Male Resident.

12/2/11 - Friday

- A warrant to search the Male Resident's home is issued and executed.
- Chief Medical Officer and Chair of Internal Medicine issues precautionary suspension of the Male Resident's patient care responsibilities, pending the outcome of the investigation. (Male Resident is a clinical trainee in a joint internal medicine/pediatrics program.)
- President Coleman is notified.

12/3/11 - Saturday

- President Coleman asks the Executive Director of University Audits to conduct an internal review, to determine the underlying control failures that caused the delay, and recommend changes.
- Executive Director of University Audits notifies Regent White, Chair of the Finance, Audit, and Investment Committee of the Board of Regents.

12/16/2011 - Friday

- The Male Resident is arrested by DPS officers.
- The Executive Committee on Clinical Affairs unanimously voted to summarily suspend the Male Resident's appointment as a clinical program trainee effective immediately.
- The University of Michigan Graduate Medical Education Office discharged the Male Resident from his Medicine-Pediatrics residency training program effective 12/16/2011.

12/17/11 - Saturday

- The Male Resident is arraigned on charges of possession of child pornography.

Addendum II

Text of e-mail sent to Data Security Analyst and HHC-Security Officer on 5/25/2011

Per our conversation, The Office of the General Counsel (OGC) would like you to pull the windows event logs from May 23rd for the computer terminal in question located in the pediatric resident room. We are interested in determining who used the computer on May 23rd and, if possible, what programs or files were accessed by each user (the “Task”).

The OGC is enlisting your assistance and delegates the necessary authority to you on behalf of the OGC to carry out various tasks that will aid the OGC in the investigation and defense of actual or anticipated litigation. All such tasks will be directed by counsel in the OGC. The objective of this engagement is to gather and review documentation related to the Task. Your principal role will be to assist legal counsel in collection and review of this information. You will inform us of any related matters that come to your attention, and all communications between you and us, shall be regarded as confidential and made solely for the purpose of assisting us in rendering legal advice, and therefore, is subject to the attorney-client privilege and the attorney work product protection. Since we are engaging you to assist us, we intend that all of the activities that you undertake pursuant to this delegation of authority also will be subject to all privileges and protections applicable to the OGC attorneys.

It may be necessary for us to disclose to you our legal theories, as well as other privileged information and attorney-work product “Confidential Information.” You agree that during and after the period of your engagement you will not disclose any Confidential Information to any person or entity to whom disclosure has not been previously authorized (in writing) by us. Please do not disclose to anyone, without our prior written permission, the nature or content of any oral or written communication with us in the course of this engagement. We ask that you communicate only with attorneys in the OGC about substantive issues, the results of your activities, or any questions that you may have.

If you have any questions regarding the above, please do not hesitate to contact me. Thank you.