THE UNIVERSITY OF
CHICAGO
HIPAA Program Office

HIPAA Program Office
Annual Report
Calendar Year 2007

Making A Difference

Date: July 1, 2008

HIPAA PROGRAM OFFICE
ANNUAL REPORT – CALENDAR YEAR 2007
MAKING A DIFFERENCE

TABLE OF CONTENTS

I. HIPAA PROGRAM OFFICE VISION AND MISSION

Vision
The University of Chicago Medical Center (UCMC) and the Office of Medical Center Compliance (OMCC) are committed to fostering a corporate culture of ethical behavior and integrity in all matters related to compliance with the Health Insurance Portability and Accountability Act (HIPAA) of 1996. Privacy is one of the values that the Medical Center's Health Care Integrity Program aspires to protect. HIPAA sets standards for the privacy and security of health data. In addition, HIPAA establishes national standards for electronic health care transactions and national identifiers for providers, health plans, and employers.

Mission
The HIPAA Program Office ("HPO") within the OMCC has been established to support the UCMC in its HIPAA compliance efforts.

The role of the HPO is to further the mission of the UCMC by serving as a resource to the institution and its patients. The HPO ***provides information and tools to support employees, faculty, and students in their efforts to ensure the privacy and security of our patients' health information. The HPO utilizes a variety of methods and initiatives to keep the workforce informed about privacy and security obligations and best practices including:***

- Monitoring all HIPAA requirements ("Rules")
- Developing HIPAA Privacy and Security policies
- Creating guidelines and procedures that make our HIPAA policies easier to follow
- Conducting ongoing workforce education and awareness activities on HIPAA privacy and security practices/principles
- Initiating ongoing auditing and monitoring activities
- Investigating privacy complaints and incidents

Being available to staff and faculty helps reassure them that they are doing the right thing as it relates to protecting patient privacy and reminds them that they are not on their own to navigate and interpret the complex HIPAA regulations. The HPO provides subject matter experts, guidance, and tools that employees can use to put their privacy awareness into action.

The core functions of the HPO are based after the seven elements of an effective compliance program as established by the United States Sentencing Commission. These elements include:

1. Written Policies and Procedures;
2. Designation of a Chief Compliance Officer and Compliance Committees;
3. Training and Education;
4. Effective Lines of Communication;
5. Enforcement of Standards;
6. Auditing and Monitoring; and
7. Responding to Detected Offenses and Developing Corrective Action

Additionally, the United States Sentencing Commission has identified several minimum standards for compliance program effectiveness including:

- Promotion of an organizational culture that encourages ethical conduct and a commitment to compliance with the law;
- Board of director responsibility for and involvement in oversight and management of compliance activities; and
- Risk assessment.

This document details the activities of the HPO for calendar year 2007. The sections that follow include a review of the HPO's efforts to illustrate how it meets the seven elements of an effective compliance program. The last section of the Annual Report is a look ahead to the activities and improvements that are expected in calendar year 2008.

II. STRUCTURE AND ACTIVITIES

A. WRITTEN POLICIES AND PROCEDURES

The UCMC has HIPAA privacy and information security policies that address requirements and issues with which it must comply under the HIPAA Privacy and Security Rules. The privacy policies were created in 2003 prior to the April 14, 2003 compliance date and the security information policies were created in 2005 in preparation for the April 20, 2005 compliance date. The information security policies were reviewed and updated in 2007 as part of the BSD HIPAA Security Remediation Project. These policies are located on the HIPAA Program Office Website (http://hipaa.bsd.uchicago.edu).

In addition to the policies, the HIPAA Program Office develops written guidances on patient privacy and confidentiality issues. The guidances are located on the HPO website. They provide direction to staff and faculty on how to apply patient privacy principles and practices on the job.

Before the guidance documents are finalized and disseminated, drafts are shared with the applicable UCMC personnel for comment and discussed with the HIPAA Frequently Asked Question (FAQ) Team comprised of representatives from the HPO, OMCC, and UCMC Legal Affairs. The HIPAA Program Director updates the HIPAA Steering Committee on the identification and status of the written guidances quarterly. In CY2007, the following documents were created or updated:

1. A to Z: HIPAA Tips for Protecting Privacy and Security
2. Accounting of Disclosures Definition Table
3. HIPAA Quick Reference Guide for Employees ***(14 page question/answer document)***
4. HIPAA Reference Sheet
5. Law Enforcement Access to Patients and PHI Guidance
6. When a Minor is Not a Minor Guidance
7. HIPAA Privacy Review Program Report Form

B. HIPAA PROGRAM OFFICE AND COMPLIANCE COMMITTEES

1. Privacy Officer

The Chief Compliance and Privacy Officer is Kerry Congdon DeMott. Ms. DeMott reports to the Dean of Clinical Affairs and has direct access to the Medical Center's President, Chief Executive Officer, and the Board of Trustees. Ms. DeMott provides updates to the Audit Committee of the UCMC Board at least once per year and regularly addresses other leadership bodies such as Senior Management Group and Divisional Executive Committee. Bob Gross, Director of the HIPAA Program Office, provides leadership in the day-to-day management of the HIPAA Program Office and staffing of the HIPAA Compliance Committees.

During 2007, the HIPAA Program Office achieved numerous milestones that are described throughout this report. Of particular note are accomplishments with respect to the infrastructure that served as the platform for the HPO's 2007 activities:

1. Conclusion of a rigorous process redesign project and full implementation of all recommendations
2. Promotion of the Manager of the HIPAA Program Office to Director
3. Recruitment of a second HIPAA Program Office Analyst

2. Compliance Committee

Members of the Senior Management Group are actively engaged in HIPAA activities. The HIPAA Steering Committee[1] and the HIPAA Security Remediation Oversight Committee[2] meet quarterly and monthly, respectively. The HIPAA Steering Committee dedicated significant time in 2007 to the development of a draft guidance for faculty and staff who use email to communicate with or about patients in a secure manner. This document is expected to be finalized and disseminated in CY2008 and will provide faculty and staff with the information and tools necessary to communicate PHI via email in a HIPAA compliant manner. The HIPAA Steering Committee meetings also served as a forum for the HIPAA Program Director to discuss or provide updates on the following programs and areas of interest:

1. HIPAA Privacy Review Program
2. Faculty and Staff Education/Awareness Initiatives
3. Written Guidances and Documents
4. Access Monitoring and Auditing Projects
5. Incident and Complaint Investigations

The HIPAA Security Remediation Oversight Committee, which is chaired by Rafael Espinosa of BSDIS, has directed three subgroups (Security Architecture, Thought Leaders, and Disaster Planning) towards completion or revision of numerous policies, procedures, and operational updates. The Oversight Committee members provide important operational expertise to the project, help to set goals, priorities, and milestones for the remediation effort, and serve as ambassadors to faculty and staff. The project required a significant amount of departmental and individual commitment and discipline, and involved meticulous documentation on assessing organizational risk, decision-making, and remediation. A well thought out methodology was developed and used to track departmental compliance with specific policy and procedure requirements. Members of the Oversight Committee and subgroups regularly followed up with the departmental contacts to ensure timeframes were met. The Project's well-documented approach, remediation plan, and monitoring activities demonstrate a good faith effort to comply with the HIPAA Security Rule. This documentation can be presented to regulatory agencies that may wish to audit the Medical Center's HIPAA Security initiatives.

In CY 2007, the Security Remediation Oversight Committee and subgroups accomplished the following:

1. Developed a compliance departmental and divisional "scorecard;"
2. Established a formal Communication Strategy for the policy review process;
3. Expanded the reference/definition of data from ePHI to "sensitive data" (this now includes research, budget, personnel, and medical information);
4. Recast the HIPAA security policies to be "information security" policies;
5. Began creating departmental written procedures and complying with the information security policies;
6. Conducted a "Data Criticality Survey" to assist with prioritizing applications/systems containing PHI for disaster planning purposes;
7. Aligned the BSD Security Remediation Project with UCMC's Security Risk Assessment activities; and
8. Hired a Project Documentation Specialist

[1] HIPAA Steering Committee Membership: Betsy Akrivos-Hoare (HPO), Kerry Congdon DeMott (HPO), Robert Gross (HPO), Ann Schwind (Dean's Office), Sandy Senti (BSDIS), Carolyn Wilson (Ambulatory Services), and Eric Yablonka (UCMCIS).

[2] HIPAA Security Risk Remediation Oversight Committee: (Jennifer Davis (BSDIS), Kerry Congdon DeMott (HPO), Tyler DeNormandie (Health Studies), Sue Eaton (Surgery), Rafael Espinosa (BSDIS), Robert Gross (HPO), Robin Honig (Dean's Office - Finance), Mike Jonen (Medicine), David Jones (BSDIS), Barb Kass (Health Studies), Kathy Kujawa (Dean's Office – Business Process), Sandy Senti (BSDIS), Ann Schwind (Dean's Office), Michele Stochl (UCPG).

C. CONDUCT EFFECTIVE EDUCATION AND TRAINING (AWARENESS) PROGRAMS

The HPO engages in a wide range of educational sessions, internal communications, and special events/programs that are designed to maintain visibility of patient privacy and information security principles and practices. These initiatives reflect, in variety and in number, the breadth and scope of education and training that is provided to UCMC employees, faculty, students, and volunteers.

The HIPAA Security Rule requires healthcare organizations to have a **security reminders program** to educate employees on essential information security behaviors and practices. The HPO addressed this requirement by employing a multi-tiered approach toward educating employees on both patient privacy principles and information security practices.

Below is more information about the HIPAA Program Office's education and awareness activities and programs:

1. Educational Sessions/Outreach Programs

As the HPO mission states, the HPO provides information and tools to support employees, faculty, and students in their efforts to ensure the privacy and security of our patients' health information. One way the HPO demonstrates this is by "being out there" interacting with members of the workforce. Reinforcing the principles and importance of protecting patient privacy and information security will help create a culture of compliance at the UCMC. In 2007, the HPO conducted numerous educational sessions and participated in organization administered programs.

1. New Employee Orientation – BSD and UCMC
2. Medical Student Orientation
3. Department of Medicine – Summer Research Programs
4. University of Chicago Police Training Sessions
5. Department of Finance – Darien Location
6. UCPG – Burr Ridge Location
7. "Best of the Best" High School Tour Groups – Office of Community Affairs
8. HIPAA Refresher Sessions – UCMC Departments and Locations **(23 in total)**

2. Internal Communications

a. Forefront Articles

The HPO published HIPAA related articles 6 times in CY2007. Additionally, the Forefront ran a picture of the HIPAA Heroes taken at the HIPAA Hero Luncheon in the June issue. Below are the publication schedule and titles of the articles:

Month	Title
January	Calling All HIPAA Heroes
March	Don't Be a Statistic – Safeguard Your Workstation
May	Playing It HIPAA Smart: Lock/LogOff Your Workstation
June	Picture of HIPAA Heroes (Taken During HIPAA Hero Luncheon)
July	Use Caution When Discussing Patient Information in Public Places
September	Resist the Urge to View Medical Records Unnecessarily
November	Use Caution When Verbally Disclosing PHI

b. HIPAA Tips of the Week – 2007

Each week, the HIPAA Program Office includes a brief HIPAA privacy or information security tip in *This Week at UCMC* online listing of events and it is also posted on the HPO website – under the "Online Feature" section. The tips focus on a variety of HIPAA issues that are also reflected in the written guidances and policies. Below are examples of topics that were covered in CY2007:

1. What can be written on a white board?
2. How to request a HIPAA refresher training
3. Faxing information to the wrong place
4. How to report a privacy or security incident/violation
5. What is PHI?
6. What is the HIPAA Program Office does the HIPAA Program Office do?
7. What to do if a current or former co-worker is a patient?
8. As an employee, may I access my own PHI?
9. What to do when a patient has a visitor in the exam room?
10. How to protect mobile devices?

c. HIPAA Privacy and Security Message of the Month Poster Campaign

In June 2007, the HPO initiated a HIPAA Privacy and Security Message of the Month Poster/email Campaign to develop greater awareness among UCMC faculty and staff. The purpose of the Campaign is to reinforce key privacy and information security practices, behaviors, and principles through the use of humor and actionable messages. This 12 month Campaign involves placing posters in highly visible locations throughout UCMC, posting key information points on the HPO website, and emailing the key points to UCMC faculty and staff. Staff and management are encouraged to post the key points in employee areas to reinforce the messages. It is anticipated that this Campaign will continue indefinitely and be assessed annually.

Below is a list of locations where posters can be viewed:

1. Mitchell Hospital Lobby
2. UCMC IS Offices – Darien – 1st and 2nd Floors
3. DCAM Cafeteria Entrance
4. UCPG Offices – Burr Ridge
5. Comer Hospital – 1st Floor
6. Windermere Senior Center
7. Comer Hospital – 2nd Floor
8. BSD IS Offices – McGiffert Hall
9. Wyler's Children's Hospital Entrance
10. UCMC RDO Offices (4 locations)
11. Goldblatt Pavilion Lobby
12. Health Information Management Department
13. Ellis Avenue Entrance
14. Medical Student Lounge
15. UCMC Finance Offices – Darien
16. HIPAA Program Office

Below is the calendar of awareness topics for CY2007 & CY2008:

Month	Topic
June - 2007	Lock/LogOff Your Computer Before Leaving Your Desk
July	Be Care Discussing PHI in Public Places
August	Incident Reporting
September	Shred Your PHI
October	Use Your Own Access Code or Card Key
November	Password Management
December	Defend Against Identity Theft

3. Special Events & Programs

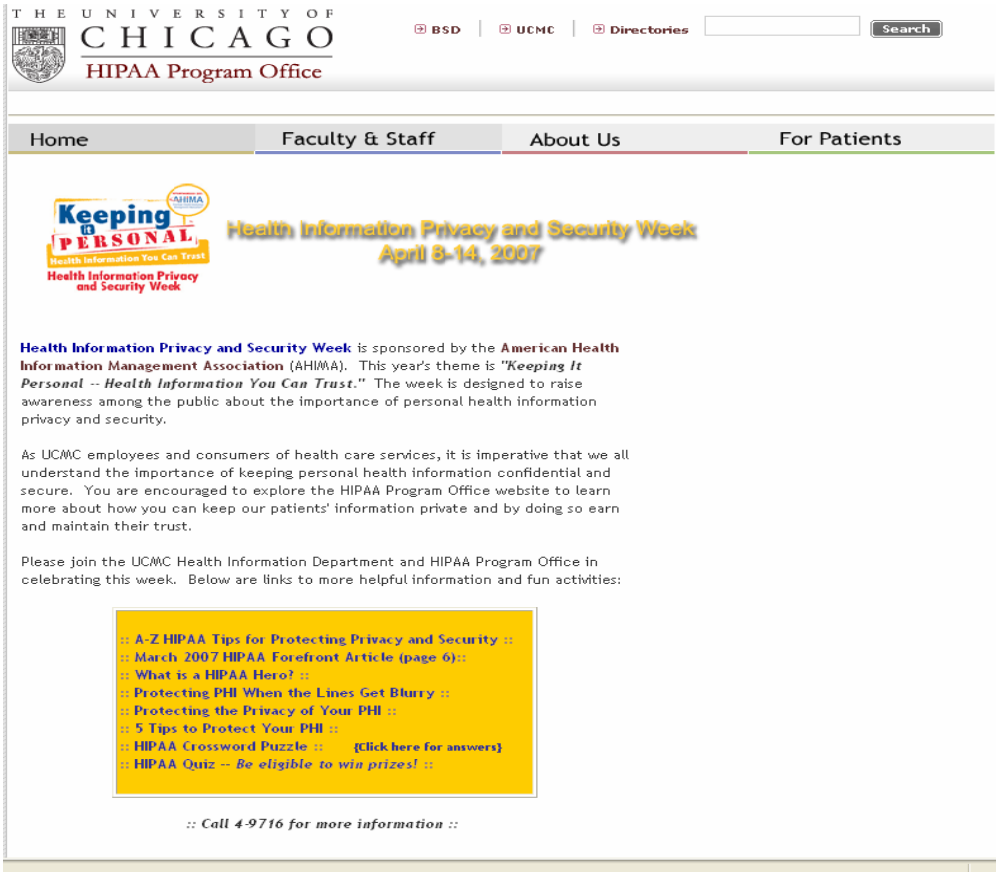
a. Health Information Privacy and Security Week - 2007

April 8-14, 2007 The University of Chicago Medical Center (UCMC) celebrated Health Information Privacy and Security Week which is an annual event sponsored by the American Health Information Management Association (AHIMA). The theme was ***"Keeping It Personal – Health Information You Can Trust."*** The week is designed to raise awareness among the public about the importance of personal health information privacy and security. The week also serves as a reminder to all UCMC staff and faculty that it is essential that we protect our patients' privacy and the confidentiality of their health and other sensitive information – not just during the week, but EVERYDAY! Incorporating patient privacy and security principles and behaviors into everything we do – patient care, operations, billing, research, and education - is essential to UCMC's success.

The HIPAA Program Office invited all staff and faculty to celebrate the week by:

- Going to the HIPAA Program Office Website (http://hipaa.bsd.uchicago.edu) and reviewing the wealth of materials on HIPAA privacy and security.
- Contacting the HIPAA Program Office at 4-9716 or HPO@bsd.uchicago.edu with questions about patient privacy and security.
- Clicking on the Website's **Health Information Privacy and Security Week** link for more information and a chance to win prizes.

Below is a picture of the Health Information Privacy and Security Week webpage on the HPO Website. Faculty and staff were informed via email about the week and encouraged to go to the website to learn more about patient privacy and information security.



Health Information Privacy and Security Week is sponsored by the **American Health Information Management Association** (AHIMA). This year's theme is ***"Keeping It Personal -- Health Information You Can Trust."*** The week is designed to raise awareness among the public about the importance of personal health information privacy and security.

As UCMC employees and consumers of health care services, it is imperative that we all understand the importance of keeping personal health information confidential and secure. You are encouraged to explore the HIPAA Program Office website to learn more about how you can keep our patients' information private and by doing so earn and maintain their trust.

Please join the UCMC Health Information Department and HIPAA Program Office in celebrating this week. Below are links to more helpful information and fun activities:

:: A-Z HIPAA Tips for Protecting Privacy and Security ::
:: March 2007 HIPAA Forefront Article (page 6)::
:: What is a HIPAA Hero? ::
:: Protecting PHI When the Lines Get Blurry ::
:: Protecting the Privacy of Your PHI ::
:: 5 Tips to Protect Your PHI ::
:: HIPAA Crossword Puzzle :: **{Click here for answers}**
:: HIPAA Quiz -- ***Be eligible to win prizes!*** **::**

:: Call 4-9716 for more information ::

b. HIPAA Hero Program

In 2007, the HPO continued its HIPAA Hero Program that it initiated in May 2006. The goal of the Program is to publicly recognize individuals who demonstrate leadership, integrity, and initiative by making a “good catch,” taking a stand, or preventing a HIPAA privacy and security incident. A program of this nature also helps educate UCMC faculty and staff on a variety of HIPAA issues with the purpose of ***“Turning Awareness Into Action.”***

These individuals are recognized for going above and beyond the duty to comply with healthcare laws, regulations, and rules that are applicable to his or her job responsibilities. For demonstrating their commitment to HIPAA compliance, they receive the following items:

1. A Certificate of Appreciation from the HIPAA Program Office;
2. HIPAA Program Office branded items; and
3. An invitation to the UCMC Compliance Luncheon celebrating HIPAA Heroes and Compliance Champions which is held during Corporate Compliance and Ethics Week.

In 2007, the HPO recognized the following individuals as HIPAA Heroes:

Nieshaa Berry (Ophthalmology)

Patricia Burns (Coagulation Lab)

Samuel Campbell (Ophthalmology)

Rafael Espinosa (BSDIS)

Tyler DeNormandie (Health Studies)

Melanie Hawkins (Radiology)

Tiana Korley (Legal Affairs)

John McGarey (Surgery)

Douglas Richardson (OBGYN)

Tony Rubino (UCMCIS)

Letitia Patterson (Ophthalmology)

D. DEVELOPING EFFECTIVE LINES OF COMMUNICATION

1. Access to the HIPAA Program Office Resources

The HPO as well as its website is available for all faculty, staff, and patients. The HIPAA Director and two HIPAA Analysts are full-time employees available to answer questions and follow up on complaints, incidents, and concerns. The Chief Compliance and Privacy Officer is also available to accept and investigate questions and concerns that have been vetted by the HPO team. Together, these four individuals serve as resources to employees and patients on issues pertaining to patient privacy, confidentiality, and data security. The HPO staff interacts daily with employees either in person or by phone and provides:

1. Verbal answers to questions that require interpretation;
2. Written guidance documents on issues employees regularly experience;
3. Tools to help facilitate compliance with the HIPAA rules;
4. A forum for employees and patients to express patient privacy concerns;
5. Influence on matters impacted by HIPAA (e.g. meeting participation); and
6. An opportunity to collaborate and facilitate on matters that need remediation.

In addition, the HPO website provides ready access to HIPAA privacy and information security policies, guidances, forms, tips, links to external resources, and ways to contact the HIPAA Program Office staff.

2. **Outreach and Interaction with Customers**
The HPO maintains visibility throughout the Medical Center by attending standing and adhoc organizational and departmental meetings for Medical Center leadership, key Medical Center programs and strategic initiatives. During these meetings, HPO representatives offer updates and guidance, make announcements, and take note of any initiative or issue requiring follow-up or monitoring.

In 2007, HPO representatives participated in the following meetings:
1. HIPAA Steering Committee
2. HIPAA BSD Risk Remediation Oversight Committee
3. UCH Billing, Coding, & Documentation Subcommittee
4. Phoenix Project Meetings
5. HIPAA FAQ Meeting
6. CACSP
7. ORIC
8. Lead Coordinators Meeting

In addition, the Chief Compliance and Privacy Officer provided updates to the Senior Management Group, Divisional Executive Committee, and Audit Committee of the Board.

3. **Development of the HPO Database**
In the first quarter of 2007 the HPO developed a business case for a central repository for all HIPAA related inquiries, complaints, incidents, and privacy review results that would be built on a secure platform. In May 2007, the HPO Director recommended, and the HIPAA Steering Committee approved, a full-featured secure database to consolidate all information, and provide robust reporting and analytical capabilities.

In June 2007, the HPO began working with BSDIS on developing the database specifications, features, and functionality and anticipate launching the database in January 2008.

E. ENFORCING STANDARDS THROUGH WELL-PUBLICIZED DISCIPLINARY GUIDELINES

Employees of the UCMC must comply with all applicable HIPAA patient privacy and information security policies. Specifically, new employees are required to sign confidentiality agreements stating that they will protect our patients' privacy in accordance to UCMC policies. In addition, consequences for violating patient privacy and confidentiality are explicitly addressed in new employee orientation and refresher training sessions. These messages are also communicated to existing employees through the various education and awareness initiatives as well as through an online message (see below) when they login to (access) UCMC information systems (e.g. OACIS).

UCH COMPUTER SECURITY/CONFIDENTIALITY AGREEMENT

As a member of the UCH community, you may access/use only those covered resources for which you have received explicit authorization. You must exercise due care to ensure that no one else learns your identification/password or has access an any physical or programmed identifications/authentication devices for information. Specifically, user ID and passwords or physical devices may not be shared among individual users. Your access code should not be :1. written down in an accessible location; 2. embedded in computer log-in scripts or other applications; or 3. stored on individual users' computers. You must exercise due care to log off the computer or terminal before leaving for a material time period to prevent anyone else from using the device under you access permissions.

You must also maintain the confidentiality of patient medical, financial and personal information. Any unauthorized or inappropriate access to or disclosure of information about a patient is a breach of medical ethics, a cause for legal action against you and a cause for disciplinary action.

Proceeding to access this application acknowledges- you have read the UCH Computer Security/Confidentiality Agreement, fully understand your responsibilities and agree to utilize all your access to UCH computer networks and systems in accordance with this agreement.

F. AUDITING AND MONITORING

1. HIPAA Privacy Review Program

The HPO mission is to promote a culture of respect for privacy and information security throughout the organization when providing patient care and accessing and disclosing protected health information. Our continuous effort to protect patient privacy and confidentiality of health information includes ongoing site visits to assess compliance with the HIPAA Privacy Rule. A site visit, called a *Privacy Review*, is an educational and consultative review that serves as a vehicle to identify best practices as well as opportunities for improvement. During the review of a location, the reviewer uses a tool called the HIPAA Privacy Review Form which includes the specific privacy standards that will be reviewed. At the end of the review process, a formal report identifying action items for remediation is generated and agreed to by the location and the HPO.

The Privacy Review program is designed to be transparent in order to maximize the opportunity to impart knowledge and effect change. It incorporates a methodology that is composed of many milestones for which timeframes and HPO service standards are defined. In 2007, the HPO reported to the HIPAA Steering Committee that the milestones and service standards were being regularly met. The program is designed to be educational rather punitive. Each review presents an opportunity to give members of the workforce the information and tools that they need to protect patient privacy. Below are the goals of the Program:

Program Goals

1. Promote a culture of respect for patient privacy
2. Monitor and confirm departments' compliance with key privacy principles
3. Identify and communicate best practices throughout the organization
4. Identify and remediate opportunities for improvement
5. Fulfill regulatory obligation and document our good faith effort to comply
6. Look for guidance and educational opportunities
7. Create a forum for staff and management to communicate privacy concerns and issues to the HPO

Program Scope and Results

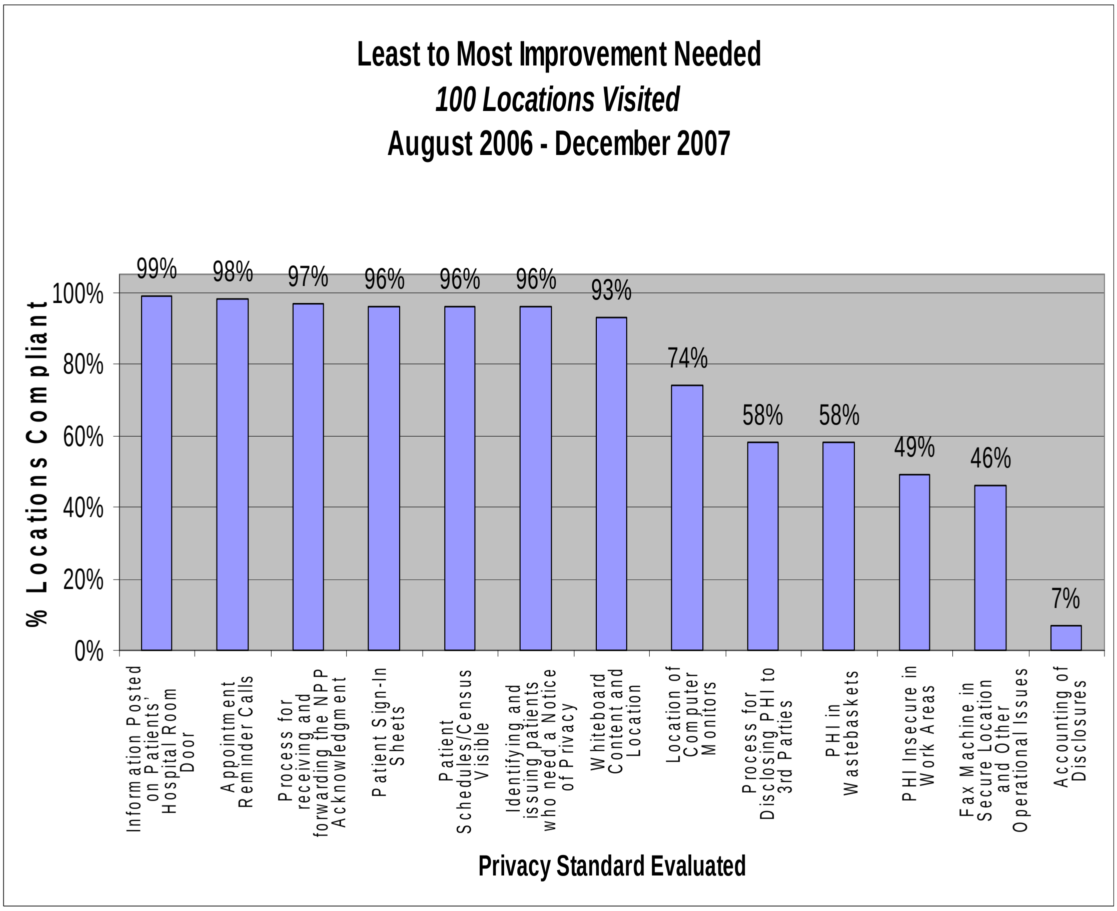
During each Privacy Review, the following areas are evaluated to determine the location's level of compliance with protecting and securing patient information:

1. Procedures
   a. Accounting of Disclosures
   b. Notice of Privacy Practices
   c. Acknowledgment Forms
   d. Appointment Reminders
   e. Disclosing PHI to 3rd Parties

2. Written Communication
   a. PHI in the Wastebasket
   b. PHI in Insecure Areas
   c. Content and Location of Whiteboards
   d. Medical Record Storage
   e. Patient Sign-in Sheets

3. Technology
   a. Computer Monitors
   b. Fax Machines
   c. Printers

Since the launch of the Privacy Review Program in August, 2006, the HPO conducted **100 privacy reviews** *(21 in 2006 and 79 in 2007)* on and off campus for administrative and clinical departments. The management and staff in each location participated in both an Entrance and Exit Conference and each location worked with the HPO to address those items identified as needing improvement. The HPO staff continued to follow up with each location to confirm that the action items were completed. The below comparative graph reflects those areas needing the least to most improvement. The Program's results help the HPO identify topics for its education/awareness activities and assist with identifying privacy and security risks and prioritizing other HPO initiatives.



2. **Employee Access to Electronic Protected Health Information**
   The HPO educates employees that they must only access PHI (e.g. electronic, hard copy) for purposes necessary to perform their own job duties, may not access and/or copy their own medical information through UCMC's information systems, including test results, clinic notes, and operative reports, and may not access through UCMC's information systems, the medical information of family members, friends, co-workers, or other individuals for personal or other non-work related purposes, even if written or oral patient authorization has been obtained. Employees who violate these guidelines are subjected to disciplinary action, up to and including termination.

   In 2007, the HPO conducted numerous OACIS access audits in response to patient allegations/complaints, incidents reported by the local media, and proactive audits around certain highly confidential diagnosis (e.g. HIV/AIDS, Mental Health). As a result of these audits, two individuals were terminated for inappropriately accessing electronic PHI. Refer to the chart in Section II G. for a complete breakdown of the types of corrective actions taken in 2007.

   It should be noted that the introduction of an electronic medical record (e.g. Phoenix Project – EPIC) increases the risk of users inappropriately accessing PHI, thus there is a greater need for proactive monitoring (not just retrospective). This has been proven, on a small scale, to be extremely time consuming. In 2007, the HPO began to work with other UCMC departments on identifying standard and adhoc user access reports that assist with the HPO's auditing and monitoring functions. Additional collaboration will take place in 2008. It is expected that more HPO resources will be allocated to conducting proactive monitoring around specific criterion – such as patient diagnosis, patient status (e.g. VIP, celebrities), and employee/co-worker or family relationships.

G. RESPONDING TO DETECTED OFFENSES AND DEVELOPING CORRECTIVE ACTION INITIATIVES

The HPO has a formal, documented process for investigating patient privacy complaints and incidents and applying appropriate sanctions to employees who do not comply. Disciplinary actions are commensurate with the degree of non-compliance and are applied after considering any extenuating circumstances related to the violation. Wherever possible, corrective action recommendations may include a training component so that the employee can advance his knowledge and understanding of patient privacy principles.

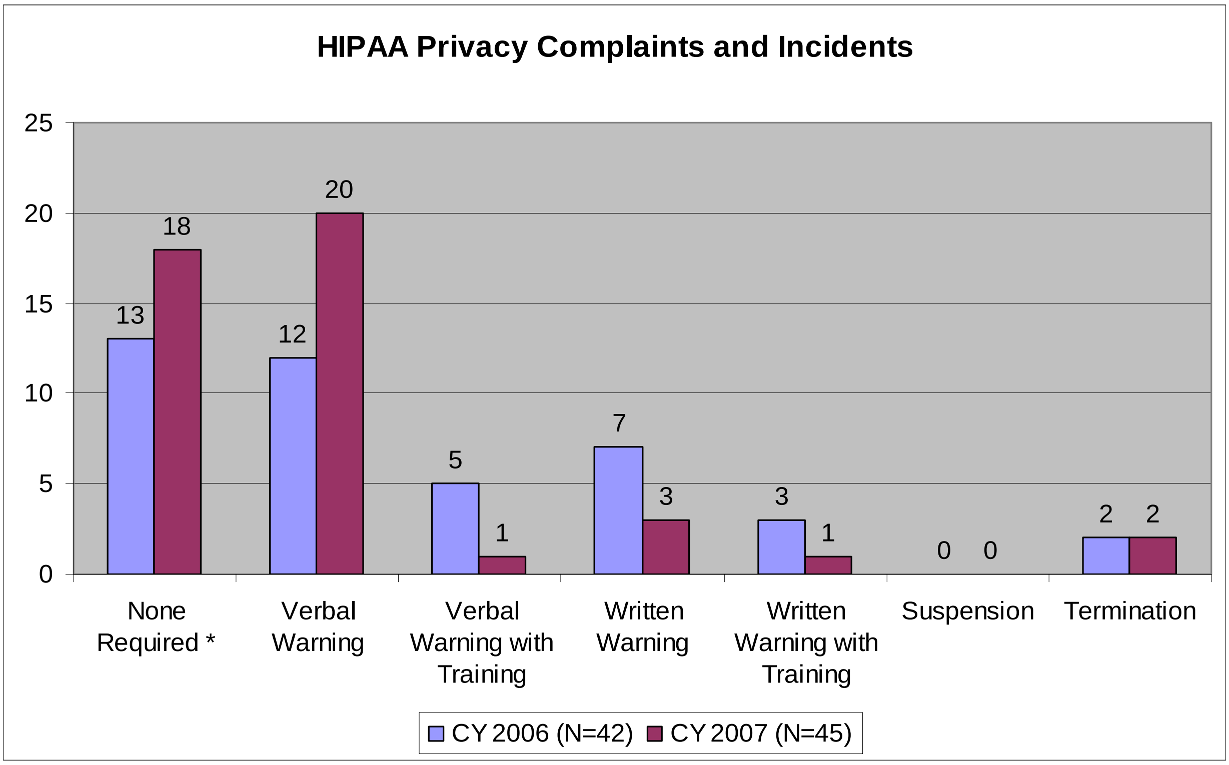
Most complaints and incidents are communicated by employees or patients directly to the HPO. Occasionally, the UCMC may receive a patient complaint from the Office for Civil Rights (OCR), the agency responsible for enforcing the HIPAA Privacy Rule. In CY2007, the UCMC did not receive a complaint from the OCR.

When the HPO is notified of an alleged violation or incident, it collaborates with the appropriate UCMC Human Resources and departmental personnel on the investigations. Investigations may include meeting with the individual(s) alleged to have violated someone's privacy, witnesses, and patients, as well as reviewing materials or information system logs. All information is documented in writing and maintained in a secure location. The HPO provides a recommendation for disciplinary action to UCMC managers and Human Resources personnel.

The following are examples of allegations/incidents that lead to investigations:

1. Inappropriate access to written or electronic protected health information (PHI).
2. Inappropriate verbal disclosure of PHI to a 3rd party.
3. Inappropriate disclosure of written PHI to a 3rd party.
4. Allegation of stealing PHI to commit identity theft.
5. Mailing PHI to the wrong patient.
6. Faxing PHI to the wrong phone number.

The below chart reflects the distribution of the corrective actions associated with the privacy complaints/incidents that took place from CY 2006 through CY 2007:



* **None Required** means that an employee or patient's observation about an incident or situation reflected in wrong perception. In other words, the investigation did not substantiate a violation, therefore no corrective action was recommended.

III. LOOK AHEAD - 2008

The HPO will continue to serve its mission by providing members of the workforce with the information and tools necessary to maintain the privacy and security of protected health information. Faculty and staff education and awareness as well as increased auditing and monitoring of privacy/security practices will be paramount in achieving this goal.

The HPO will continue to leverage existing activities and identify new opportunities to enhance its HIPAA Awareness Program. The goal of providing helpful information and tools to our employees to create a corporate culture aimed at ***"turning awareness into action"*** will serve as the motivation for all our activities. The HPO will also organize its time and focus around the goal of identifying risk areas and work collaboratively with UCMC staff and management on mitigating those risks. The HPO will continue to manage the "above the fold" risk so that UCMC does not see its name in the local and/or national media related to a HIPAA privacy and/or security breach.

A. Privacy and Security Best Practices Online Library

The first quarter of 2008 will be devoted to designing an online Best Practices Library accessed via the HPO website. One way to foster a corporate culture that promotes and reinforces patient privacy and information security principles and practices is to identify "Best Practices" and share them with UCMC departments and locations. Best Practices are tools such as signs, flyers, labels, stickers, checklists, or procedures. They are intended to further assist UCMC in its HIPAA compliance efforts and to help promote consistent ways that UCMC departments, clinics, and locations can protect patient privacy and confidentiality without having to "reinvent the wheel." It is expected that the library will launch in mid-2008 and new items will be added monthly.

B. Mandatory HIPAA Training

In 2008, the HPO will develop a strategy for conducting a mandatory all faculty and staff HIPAA training program to be implemented in CY2009. The HIPAA Privacy and Security Rules do not require employees to receive HIPAA training annually. However, the last time UCMC employees underwent mandatory HIPAA Privacy or Security training was in 2003 and 2005 respectively. The mandatory training requirement coupled with the other educational/awareness activities will further promote a corporate culture of ethical behavior related to protecting patient privacy and information security.

C. Phoenix Project – User Access to PHI

In 2008, phases of the Phoenix Project will be implemented, thus giving users greater access to ePHI. The HPO will work with UCMC IS personnel to develop standardized and adhoc reports to assist with monitoring of employees' access to ePHI. The HPO Director will develop an **auditing program** to monitor employee access to ePHI to ensure that our patients' privacy and information are protected.

D. BSD and UCMC HIPAA Security Remediation Activities

In 2008, the consolidation of the BSD and UCMC IS departments will create a need for the HPO to provide greater coordination on HIPAA security issues including but not limited to the following: risk remediation action items, information security policy adoption, user auditing/monitoring, and future risk assessment activities. The HIPAA Director will meet regularly with the UCMC IS Security Director to develop a plan for addressing UCMC HIPAA security risks.

E. Privacy Review Program – Second Round

In 2008, the HPO will begin a new round of Privacy Reviews. The HPO will reassess the Program's methodology and information to determine if modifications are needed. The HPO will decide, among other items, if the specific privacy standards need to be revised, new standards need to be added, and if the paper documents (e.g handouts) should be replaced with electronic versions.

F.. Formalization of the HIPAA Hero Program

In January 2008, the HPO and the Office of Medical Center Compliance (OMCC) will kick-off its HIPAA Heroes and Compliance Champions Program to accept nominations from faculty and staff for this special honor. Previously, individuals were recognized by the HPO and OMCC. A HPO/OMCC selection committee will be formed and all nominees will be considered on a monthly basis. Photographs of the recipients will be posted in the HPO and OMCC display cases and on their respective websites.

G. Communication Strategy

The HPO will explore with the Communications and Marketing Department opportunities to more effectively communicate privacy and security information to the UCMC workforce. This will include examining the appropriateness of the HPO's methods/channels of communication to the actual messages being communicated.