University of Pittsburgh
School of Pharmacy
Customer Information Security Plan
September 2016

Introduction

This information security plan describes the School of Pharmacy's ongoing efforts, in conjunction with the University of Pittsburgh, to secure information related to students, faculty, staff, alumni, and others who provide sensitive information to the University.

Purpose

- To ensure the security and confidentiality of customer information;
- To protect against anticipated threats to the security and/or integrity of customer information;
- To guard against unauthorized access to, or use of, customer information that could result in harm or inconvenience to any customer; and
- To comply with the Gramm-Leach-Bliley Act

Scope

This plan applies to any record containing non-public financial information about a customer who has a relationship with the School, whether in paper, electronic or other form that is handled or maintained by the School of Pharmacy.

Definitions

Customer – any individual who receives a service from the School of Pharmacy and who, in the course of receiving that financial service, provides the School of Pharmacy with non-public financial information about themselves.

Customer information – any non-public financial information about a customer that is handled or maintained by the School of Pharmacy.

Service Provider – any person or entity that receives, maintains, processes, or otherwise is permitted access to School of Pharmacy customer information through a provision of services.

Information Safeguards

A. Securing information

CONTROL ACCESS TO ROOMS AND FILE CABINETS WHERE PAPER RECORDS ARE KEPT

- Doors to office areas are locked during non-business hours.
- Customer information is processed in work areas that are behind locked doors or in other areas not regularly accessible to the general public.
- Guests are escorted in areas where customer information is being processed and are restricted to areas where customer information is not in plain view.

- File cabinets used to store customer information are secured in locked areas or areas not regularly accessible to the general public.
- Documents no longer needed are disposed of in locked shredding containers in accordance with University policy and the law.
- Key access is provided to only those individuals with appropriate clearance who require access as a result of their job responsibilities.

Control Access to Information Stored Electronically

- Computer workstations accessing customer information are to be housed behind locked doors or in areas where output devices (screens, printers, etc) cannot be seen by the general public.
- Server room is locked and School of Pharmacy servers reside in a locked cabinet. Only two staff members have access to server cabinets.
- Computer screens displaying customer information are to be minimized when not in use to prevent inadvertent breeches.
- Strong passwords are to be used. Account password changes are required upon first login. As the University sets requirements for password changes, the School of Pharmacy will implement these requirements. Currently, password changes are required twice a year.
- All School of Pharmacy computing resources are behind the University of Pittsburgh firewall.
- User IDs and passwords are not to be posted near or on computers.
- All School of Pharmacy laptops have Computrace installed as per CSSD guidelines.
- School of Pharmacy computer lab machines are equipped with Kensington locks to prevent theft.

Protecting Customers' Information

- Requests for customer information are responded to in accordance with FERPA guidelines.
- Fraudulent attempts to obtain customer information are reported to administration, who will then report the attempt to the appropriate law enforcement agency.
- All calls and mail requesting customer information are referred to individuals who have been trained in safeguarding information.
- Shredding and erasing customer information when no longer needed is done in compliance with University policy.
- The School of Pharmacy discourages the use of social security numbers and uses social security numbers only in accordance with University policy.
- The School of Pharmacy does not retain credit card data. On-line registration forms for School of Pharmacy alumni events are designed in accordance to University eCommerce guidelines and the system is tested yearly. The School of Pharmacy utilizes PayPal and Wufoo for processing of credit card registrations. Full customer credit card information is not made available to individuals processing registrations.

B. Training

The School of Pharmacy requires employees to maintain the confidentiality of University records, including financial records, of students, faculty and staff. Employees are expected to protect all confidential and proprietary information by safeguarding it when in use, filing it properly when not in use, and discussing it only with those who have a legitimate business need to know. Violations of this duty of confidentiality can lead to disciplinary action up to and including termination.

Training For Staff Members with Access to Customer Information

- Curran Center For Pharmacy Students staff members attend training on the Family Educational Rights and Privacy Act (FERPA) offered by the University. The staff are also aware that the University's Registrar maintains an easy to read interpretation of FERPA as it applies to students' accounts at: http://www.registrar.pitt.edu/ferpa.html
- New users to PeopleSoft must receive the Introduction to PeopleSoft training offered by the University. User training increases for additional data access authority.

Information Technology Staff

- All IT staff members are educated on University policies related to securing data and information. An annual contract with CSSD ensures up-to-date information regarding policies.

Training of Other Administrative Staff

- All administrative staff sign an agreement affirming that they read and understand the University Customer Information Security Plan, inclusive of processes to assure student information confidentiality.

C. Monitoring and Detection

Utilizing University Resources

- The School of Pharmacy has a contract with CSSD. The CSSD analysts evaluate the existing computing systems and safeguards to ensure they meet University requirements and make necessary recommendations for improvements.
- The University of Pittsburgh Internal Audit Department requires an annual review of the Control Self Assessment certification. Any changes to our procedures relevant to customer information must be documented as a result of this annual review.

Internal Safeguards

Appropriate University police and/or administrators are contacted in the event of any red flags. Red flags include but are not limited to:

- Receipt of alerts from consumer reporting agencies.

- Receipt of suspicious documents containing forged signatures or apparent alterations or an identification card with a photograph that does not resemble the owner of the account.
- Receipt of suspicious personal identifying information such as Peoplesoft number that does match the student, or information that matches somebody else's education records, or submitting a lack of required personal information after further request.
- Unusual use of or other suspicious activity related to an account.
- Receipt of notices from victims, law enforcement agencies, or others.

Employees are encouraged to report suspicious activity to supervisors and law enforcement authorities.

The Customer Information Security Plan is reviewed annually. Selected aspects will be tested and monitored to ensure the plan's safeguards remain current and effective. Updates will be made as necessary.

THIRD-PARTY VENDORS

- The School of Pharmacy only selects third party service (PayPal and Wufoo) with providers that are capable of maintaining appropriate safeguards for customer information to which they will have access.

- The School of Pharmacy shall require, by contract, service providers who have access to customer information to implement and maintain appropriate safeguards for customer information.

D. **Managing Systems Failures and Handling Red Flags**

SYSTEM BACK-UPS

Data residing on the School of Pharmacy servers are backed up on a regular basis. Most critical Pharmacy data is stored on university servers at the network operations center. The school also has physical servers in the network operations center. The NOC staff handles data backup for the aforementioned systems. The remaining Pharmacy servers at Salk Hall are backed up to tape. Full backups are done Friday night through Monday morning. Those same tapes are then used for the differential backups done Monday through Thursday evenings. Tapes are taken offsite.
The School of Pharmacy is committed to moving all applicable computing services to the Network Operations Center and is in the process of moving remaining websites to the University Enterprise Web Infrastructure.

SECURITY BREACHES

In the event that information security is compromised, a prompt disclosure will be made to any customers that may have been impacted and appropriate University police and administrators are contacted.

E. No Third-Party Rights

While this plan is intended to promote the security of information, it does not create any consumer, customer, or other third-party rights or remedies, or establish or increase any standards of care that would otherwise not be applicable.

F. University Policies and Procedures

All guidelines outlined in the School of Pharmacy Customer Information Security Plan are subject to compliance with University of Pittsburgh policies and procedures that protect customer information. The University of Pittsburgh policies and guidelines related to customer information can be reviewed at: http://www.provost.pitt.edu/documents/Information_Security_Plan.pdf