UNIVERSITY OF KENTUCKY

Office of Legal Counsel
Main Campus Location
301 Main Building
Lexington, KY 40506-0032
859 257-2936
fax 859 323-1062
www.uky.edu/Legal

Office of Legal Counsel
Medical Center Location
317 Charles T. Wethington Building
Lexington, KY 40536-0200
859 323-1161
fax 859 257-5123
www.uky.edu/Legal

MEMORANDUM

To: **University of Kentucky Executive Vice Presidents, Deans, and Department Heads**

From: **William E. Thro**
General Counsel

Date: **December 1, 2014**

Re: **New Security, Breach Notification and Contract Language Requirements**

I. Executive Summary

On January 1, 2015, a new state law, the Personal Information Security and Breach Investigation Procedures and Practices Act ("Act") goes into effect. This Act concerns the protection of personal information and applies to every state agency and university. This memorandum addresses three requirements of the new law: contracts, initial breach notification procedures and data security.

Please share this information as needed within your unit.

A. Contracts. For all agreements the University executes or amends on or after January 1, 2015, with a third party to whom the University discloses "personal information" (defined below), the following provision shall be included in those agreements:

> To the extent Company receives Personal Information as defined by and in accordance with Kentucky's Personal Information Security and Breach Investigation Procedures and Practices Act, KRS 61.931, 61.932 and 61.933 (the "Act"), Company shall secure and protect the Personal Information by, without limitation: (i) complying with all requirements applicable to non-affiliated third parties set forth in the Act; (ii) utilizing security and breach investigation procedures that are appropriate to the nature of the Personal Information disclosed, at least as stringent as University's and reasonably designed to protect the Personal Information from unauthorized access, use, modification, disclosure, manipulation, or destruction; (iii) notifying University of a security breach relating to Personal Information in the possession of Company or its agents or subcontractors within seventy-two (72) hours of discovery of an actual or suspected breach unless the exception set forth in KRS 61.932(2)(b)2 applies and Company abides by the requirements set forth in that exception; (iv) cooperating with University in complying with the response, mitigation, correction, investigation, and notification requirements of the Act , (v) paying all costs of notification, investigation and mitigation in the event of a security breach of Personal Information suffered by Company; and (vi) at University's discretion and direction, handling all administrative functions associated with notification, investigation and mitigation.

The term "Company" may be revised to fit your respective contract templates or agreements.

seeblue.
An Equal Opportunity University

Questions regarding this contract language should be directed to the Office of Legal Counsel.

B. Breach Notification Procedures. Any known, suspected or alleged unauthorized acquisition, distribution, disclosure, destruction, manipulation or release of personal information (hereafter "Incident") shall be reported immediately to the Security Breach Reporting Line (by calling **(859) 218-3904**), UK HealthCare Corporate Compliance Office (by calling **(859) 323-8002**), or UK HealthCare ITS Help Desk (by calling **(859) 323-8586**). Incidents involving protected health information or personal information containing protected health information shall be reported to UK HealthCare Corporate Compliance Office (by calling **(859) 323-8002)** or UK HealthCare ITS Help Desk (by calling **(859) 323-8586**).

C. Data Security. Under the new state law, the University must implement, maintain and update security procedures and practices, including appropriate corrective action, to protect and safeguard against security breaches. Thus, the University must ensure that all personal information, however stored, is protected from unauthorized access. Every UK College, department, school, institute and center must work to ensure that appropriate IT protections are in place that, at a minimum, are in accordance with security standards and requirements established by the Executive Vice President for Health Affairs (EVPHA) Technology Office for units falling under EVPHA and University of Kentucky Analytics and Technology (UKAT) for all other units within the University. The appropriate administrator within each UK College, department, school, institute and center must work to develop and update these security procedures and practices so that, at a minimum, those procedures and practices are in accordance with the security standards and requirements established by the EVPHA Information Technology Office for units falling under EVPHA and UKAT for all other units within the University. Other forms of storage (paper, portable devices, etc.) should also be assessed and secured accordingly.

For any questions regarding appropriate safeguards outside of UK HealthCare, please contact the Office of the Chief Information Security Officer at security@uky.edu. Questions relating to appropriate safeguards within UK HealthCare shall be directed to UK HealthCare Information Security (by calling **(859) 323-1804**).

II. Discussion

In the 2014 legislative session, the General Assembly passed the Personal Information Security and Breach Investigation Procedures and Practices Act ("Act") concerning the protection of personal information, which applies to every state agency and university. *See* KRS 61.931 et seq.

KRS 61.932(1)(a) requires that "an agency that maintains or otherwise possesses personal information, regardless of the form in which the personal information is maintained, shall implement, maintain, and update security procedures and practices, including taking any appropriate corrective action, to protect and safeguard against security breaches."

"Personal information" is defined as "an individual's first name or first initial and last name; personal mark; or unique biometric or genetic print or image, in combination with one (1) or more of the following data elements:

a. An account number, credit card number, or debit card number that, in combination with any required security code, access code or password, would permit access to an account;
b. A Social Security number;
c. A taxpayer identification number that incorporates a Social Security number;

d. A driver's license number, state identification card number or other individual identification number issued by an agency;
e. A passport number or other identification number issued by the United States government; or
f. Individually Identifiable Information as defined in 45 C.F.R. sec. 160.013 (of the Health Insurance Portability and Accountability Act), except for education records covered by the Family Educational Rights and Privacy Act, as amended 20 U.S.C. sec 1232g."

KRS 61.931(6).

According to the Act, "any agency or non-affiliated third party that maintains or otherwise possesses personal information, regardless of the form in which the personal information is maintained shall implement, maintain and update security procedures and practices, including, taking any appropriate corrective action, to protect and safeguard against security breaches." KRS 61.932(1). Additionally, state agencies and non-affiliated third parties are required to make certain notifications within certain timeframes established by the Act in the event of a determination or notification of a security breach of personal information.[1] KRS 61.932 and 61.933.

A non-affiliated third party means "any person or entity that has a contract or agreement with the University and receives [accesses, collects or maintains] personal information from the [University] pursuant to the contract or agreement." KRS 61.931(5).

To ensure the Act's requirements are met by a non-affiliated third party who may access, receive, collect or maintain the University's personal information, the Act requires all University agreements with non-affiliated third parties executed or amended after January 1, 2015 to require "the non-affiliated third party implement, maintain, and update security and beach investigation procedures that are appropriate to the nature of the information disclosed, that are at least as stringent" as the security and breach investigation procedures and practices implemented and maintained by the University "and that are reasonably designed to protect the personal information from unauthorized access, use, modification, disclosure, manipulation or destruction." Accordingly, the contract language set forth in the Executive Summary above shall be included in all agreements where the contracted party shall access, receive, collect or maintain personal information. Given the broad definition of personal information, the types of agreements requiring this language may include, without limitation, information security software licenses/agreements, vendor purchasing agreements, personal service or administrative contracts, letters, grants, research projects, memoranda of understanding or any other type of contract or arrangement where the University shares personal information with a non-affiliated third party.

If you have any questions or need additional information, please contact the Office of Legal Counsel.

[1] Specifically, absent law enforcement delay, within seventy-two (72) hours of determination or notification of a security breach (as defined by the Act), notification shall be provided to the State Police, Auditor, Attorney General and Council on Postsecondary Education. The agency also shall conduct an investigation to determine if the breach has resulted in or is likely to result in a misuse of information. Upon conclusion of the investigation if a breach has occurred and the misuse of information has or is likely to occur, the agency shall notify within forty-eight (48) hours of completion of the investigation the State Police, Auditor, Attorney General, Council on Postsecondary Education and Library of Archives. Within thirty-five (35) days after such notifications, the affected individuals shall be notified and if the number of affected individuals exceeds one thousand (1000), notification shall be made to the Council on Postsecondary Education and all consumer reporting agencies within seven (7) days prior to individual notification. KRS 61.932 and 61.933. University compliant policies and procedures are being developed.