University at Buffalo
The State University of New York

January 21, 2014

Dear Colleagues,

The University at Buffalo follows a data custodian model to exercise positive control over our important data assets ("data") (see Information Security Data Access and Security Policy). In this model, individuals who need access to institutional data are required to request access based on legitimate business needs and follow processes and methods identified by the university to request access. Upon request approval the data must be handled according to University safe data handling guidelines .

We follow this model to limit institutional risk by ensuring that decision-making is vested in the people with compliance responsibility for the data. Both University policy and state and federal regulations require that data be used responsibly and for approved purposes only. The University adheres to regulations like HIPPA and FERPA (where applicable) to dictate under what circumstances data may be shared and with whom.

Given the size and variety of our institution, it is not unexpected that people with access to specific data may have a legitimate need to use it in ways that are outside of the scope of their original request, which may include sharing the data with others that were not part of the original request. When this need occurs, it is necessary to request explicit permission for the new use case. Each request must be considered in the context of the type of data being shared (see Data Classification Standard), what types of limitations may be placed on how it is shared, and the information security maturity of the environment, department, or outsourced company that it is being potentially shared.

The need to request explicit permission for the new use case is especially important when sharing the data with non-UB hosted or owned entities (e.g., vendors, contract application service providers, "cloud" companies, etc.) in order to utilize or integrate UB information assets into their products. Non-UB hosted service providers offer new and not yet fully understood risks to our institution. It is imperative that the data custodians be involved in any decision to share outside the normal UB enterprise data and application solutions. It is also vital that we use strong, standardized contract language in all agreements that will protect both UB as well as the persons who are entrusting their private information to us.

At the bottom of this memo is recommended language from the SUNY and the Office of General Counsel that should be attached to any contract prior to sharing data with a partner.

Regards,

Jeff Murphy
Interim Information Security Officer

Guidance: SUNY procedure # 7553 Section II.D.5

g) The Federal Trade Commission (FTC) promulgated the Safeguards Rule pursuant to the Gramm-Leach-Bliley Act to insure the security and confidentiality of customer records and information emanating from such customer's receipt of a campus' financial product or service (i.e., loans or "affinity" credit cards). Campuses must require service providers by contract to implement and maintain safeguards of nonpublic personal information they possess. Relevant contracts that campuses enter into must include the required safeguarding provision:

"In performing any resulting contract, you will receive, maintain, process or otherwise will have access to confidential information on students and/or customers (Name of Campus). Pursuant to the Gramm-Leach-Bliley Act (P.L. 106-102) and the Federal Trade Commission's Safeguards Rule (16 CFR Part 314), you must implement and maintain a written Information Security Program in order to protect such customer information. Customer Information is defined in relevant part under the Safeguards Rule as 'any record containing nonpublic personal customer information as defined in 16 CFR §313(n)' (the FTC's Privacy Rule)' about a customer of a financial institution, whether in paper, electronic, or other form' (16 CFR §314.2). Examples of nonpublic personal customer information include, but are not limited to, name, address, phone number, social security number, bank and credit card account numbers and student identification numbers.

The safeguards that you implement under the Program must comply with the elements set forth in 16 CFR §314.4 and must achieve the objectives enunciated in 16 CFR §314.3, namely to: 1) insure the security and confidentiality of student and/or campus customer records and information; 2) protect against any anticipated threats or hazards to the security or integrity of such records; and 3) protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any student and/or campus customer.

If you subcontract with a third party for any of the services that you are required to undertake in furtherance of this contract, you must ensure that such third parties implement practices, which protect nonpublic personal information of students and/or campus customers with which they receive, maintain, process or otherwise are permitted access.

You are required to (return) or (destroy) (Campus to choose method) all customer information in your possession upon your completion of this contract. Furthermore, the safeguarding requirements set forth above shall survive termination of this contract."

h) The following language should be included in contracts in which the offerer will have access to nonpublic personal information: "Contractor shall comply with the provisions of the New York State Information Security Breach and Notification Act (General Business Law Section 899-aa; State Technology Law Section 208). Contractor shall be liable for the costs associated with such breach if caused

by Contractor's negligent or willful acts or omissions, or the negligent or willful acts or omissions of Contractor's agents, officers, employees or subcontractors."

Guidance: SUNY Office of General Counsel

OGC suggests using this contract clause.

> The Contractor hereby acknowledges and agrees to use commercially reasonable efforts to maintain the security of private information (as defined in the New York State Information Security Breach and Notification Act, as amended "ISBNA"(General Business Law § 889-aa; State Technology Law § 208) that it creates, receives, maintains or transmits on behalf of SUNY and to prevent unauthorized use and/or disclosure of that private information; and implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of electronic private information that it creates, receives, maintains or transmits on behalf of SUNY("SUNY Data"). The Contractor hereby acknowledges and agrees to fully disclose to SUNY pursuant to the ISBNA, and any other applicable law any breach of the security of a system where the Contractor creates, receives, maintains or transmits private information on behalf of SUNY following discovery or notification of the breach in the system as to any resident of New York State whose private information was, or is reasonably believed to have been acquired by a person without valid authorization ("Security Incidents"). The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system. The Contractor shall be liable for the costs associated with such breach if caused by the Contractor's negligent or willful acts or omissions, or the negligent or willful acts or omissions of the Contractor's agents, officers, employees or subcontractors. In the event of a Security Incident involving SUNY Data pursuant to the ISBNA, SUNY has an obligation to notify every individual whose private information has been or may have been compromised. In such an instance, the Contractor agrees that SUNY will determine the manner in which such notification will be provided to the individuals involved pursuant to the ISBNA and agrees to indemnify SUNY against any cost of providing any such legally required notice. Upon termination or expiration of this Agreement, the Contractor will follow SUNY's instructions relating to any SUNY Data remaining in the Contractor's possession. Upon authorization from SUNY, the Contractor will use data and document disposal practices that are reasonable and appropriate to prevent unauthorized access to or use of SUNY Data and will render the information so that it cannot be read or reconstructed.