Suggested Contractual Provisions for the External Sharing of University Information Classified as Level 1 Protected or Level 2 Private

Florida State University

Information Security & Privacy Office

2014

Florida State University
Information Security and Privacy Office (ISPO)

It is the responsibility of the campus unit to ensure adequate safeguarding provisions are incorporated in contracts that include any external sharing of "Protected" or "Private" FSU data (See the FSU Data Classification Guidelines and FSU Policy OP-A-6 Purchasing). Some contracts for third-party outsourcing may require explicit provisions to meet safeguarding requirements as specified in law, rule, FSU policy, or contractual obligation.

The inclusion of the provisions below should be reviewed by University legal counsel prior to signature of any contract.

Section A – Common Contract Provisions for the Any External Sharing of "Private" or "Protected" Data
Section B – Special Contract Requirements to meet Law, Regulation, or Contractual Obligations

---

Section A – Common Contract Provisions for Any External Sharing of "Private" or "Protected" Data

I. PROTECTED INFORMATION

Service Provider acknowledges that its performance of Services under this Agreement may involve access to confidential University information including, but not limited to, personally-identifiable information, student records, protected health information, or individual financial information (collectively, "Protected or Private Information") that is subject to state or federal law/rules restricting the use and disclosure of such information, including, but not limited to; the federal Gramm-Leach-Bliley Act (15 U.S.C. §§ 6801(b) and 6805(b)(2)); the federal Family Educational Rights and Privacy Act (20 U.S.C. § 1232g); and the privacy and information security aspects of the Administrative Simplification provisions of the federal Health Insurance Portability and Accountability Act (45 CFR Part 160 and Subparts A, C, and E of Part 164); the Payment Card Industry Data Security Standards . Service Provider agrees to comply with all applicable federal and state laws restricting the access, use and disclosure of Protected Information. Service Provider agrees to include all of the terms and conditions contained in all subcontractor or agency contracts providing services under this Agreement.

II. COMPLIANCE WITH FAIR INFORMATION PRACTICE PRINCIPLES

With respect to the University's Protected or Private Information, and in compliance with all applicable laws and regulations, Service Provider shall comply in all respects reasonably pertinent to the Agreement with the *Fair Information Practice Principles*, as defined by the U.S. Federal Trade Commission (http://www.ftc.gov/reports/privacy3/fairinfo.shtm). If collecting Protected or Private Information electronically from individuals on behalf of the University, Service Provider shall utilize a privacy statement or notice in conformance with such principles (the University's sample Privacy Statement for websites is available at http://fsu.edu/misc/policy.html).

III. PROHIBITION ON UNAUTHORIZED USE OR DISCLOSURE OF PROTECTED INFORMATION

Service Provider agrees to hold the University's Protected or Private Information, and any information derived from such information, in strictest confidence. Service Provider shall not access, use or disclose Protected or Private Information except as permitted or required by the Agreement or as otherwise authorized in writing by University, or applicable laws. If required by a court of competent jurisdiction or an administrative body to disclose Protected of Private Information, Service Provider will notify University in writing immediately upon receiving notice of such requirement and prior to any such disclosure, to give University an opportunity to oppose or otherwise respond to such disclosure (unless prohibited by law from doing so). Any transmission, transportation or storage of Protected or Private Information outside the United States is prohibited except on prior written authorization by the University.

IV. SAFEGUARD STANDARD

Service Provider agrees to protect the privacy and security of University data designated as Protected or Private Information according to all applicable laws and regulations, by commercially-acceptable standards, and no less rigorously than it protects its own confidential information. Service Provider shall implement, maintain and use appropriate administrative, technical and physical security measures to preserve the confidentiality (authorized access), integrity and availability of the Protected or Private Information. While Service Provider has responsibility for the Protected or Private Information under the terms of this agreement, Service Provider shall ensure that such security measures are regularly reviewed and revised to address evolving threats and vulnerabilities.

- All facilities used to store and process Protected or Private Information will employ commercial best practices, including appropriate administrative, physical, and technical safeguards, to secure such data from unauthorized access, disclosure, alteration, and use. Such measures will be no less protective than those used to secure Service Provider's own data of a similar type, and in no event less than reasonable in view of the type and nature of the data involved.

- Without limiting the foregoing, Service Provider warrants that all Protected or Private Information will be encrypted in transmission (including via web interface) and may require encrypted storage at no less than 128bit level encryption.

- Service Provider will use industry standard and up-to-date security tools and technologies such as antivirus protections and intrusion detection methods in providing Services under this Agreement.

Service Provider shall not store or process University Protected or Private Information outside of data centers located in the United States.

V. RETURN OR DESTRUCTION OF PROTECTED INFORMATION

Within 30 days of the termination, cancellation, expiration or other conclusion of the Agreement, Service Provider shall return the Protected or Private Information to University in an agreed upon format, unless the University requests in writing that such data be destroyed. This provision shall also apply to all Protected or Private Information that is in the possession of subcontractors or agents of

Service Provider. Such destruction shall be accomplished by "purging" or "physical destruction" in accordance with commercially reasonably standards for the type of data being destroyed (e.g., *Guidelines for Media Sanitization*, NIST SP 800-88). Service Provider shall certify in writing to University that such return or destruction has been completed.

VI. BREACHES OF PROTECTED INFORMATION

Definition. For purposes of this article, the term, "Breach," has the meaning given to it under the applicable Florida (F.S. 501.171) or federal law.

Reporting of Breach. Immediately upon discovery of a confirmed or suspected Breach, Service Provider shall report both orally and in writing to the University. In no event shall the report be made more than two (2) business days after Service Provider knows or reasonably suspects a Breach has or may have occurred. In the event of a suspected Breach, Service Provider shall keep the University informed regularly of the progress of its investigation until the uncertainty is resolved.

Service Provider's report shall identify:

(i) The nature of the unauthorized access, use or disclosure,
(ii) The Protected or Private Information accessed, used or disclosed,
(iii) The person(s) who accessed, used and disclosed and/or received Protected or Private Information (if known),
(iv) What Service Provider has done or will do to mitigate any deleterious effect of the unauthorized access, use or disclosure, and
(v) What corrective action Service Provider has taken or will take to prevent future unauthorized access, use or disclosure.
(vi) Service Provider shall provide such other information, including a written report, as reasonably requested by University.

Coordination of Breach Response Activities. In the event of a Breach, Service Provider will:

- Immediately preserve any potential forensic evidence relating to the breach;
- Promptly (within 2 business days) designate a contact person to whom the University will direct inquiries, and who will communicate Service Provider responses to University inquiries;
- As rapidly as circumstances permit, apply appropriate resources to remedy the breach condition, investigate, document, restore University service(s) as directed by the University, and undertake appropriate response activities;
- Provide status reports to the University on Breach response activities, either on a daily basis or a frequency approved by the University;
- Coordinate all media, law enforcement, or other Breach notifications with the University in advance of such notification(s), unless expressly prohibited by law;
- Make all reasonable efforts to assist and cooperate with the University in its Breach response efforts; and
- Ensure that knowledgeable Service Provider staff are available on short notice, if needed, to participate in University-initiated meetings and/or conference calls regarding the Breach.

Costs Arising from Breach. In the event of a Breach by the Service Provider or its staff, Service Provider agrees to promptly reimburse all costs to the University arising from such Breach, including but not limited to costs of notification of individuals, establishing and operating call center(s), credit monitoring and/or identity restoration services, time of University personnel responding to Breach, civil or criminal penalties levied against the University, attorney's fees, court costs, etc. Any Breach may be grounds for immediate termination of this Agreement by the University.

VII. EXAMINATION OF RECORDS

University shall have access to and the right to examine any pertinent books, documents, papers, and records of Service Provider involving transactions and work related to this agreement until the expiration of five years after final payment hereunder. Service Provider shall retain project records for a period of five years from the date of final payment.

VIII. ASSISTANCE IN LITIGATION OR ADMINISTRATIVE PROCEEDINGS

Service Provider shall make itself and any employees, subcontractors, or agents assisting Service Provider in the performance of its obligations under the Agreement available to University at no cost to University to testify as witnesses in the event of an unauthorized disclosure caused by Service Provider that results in litigation or administrative proceedings against University, its directors, officers, agents or employees based upon a claimed violation of laws relating to security, privacy or arising out of this agreement.

IX. SURVIVAL

The Service Provider shall maintain an industry standard disaster recovery program to reduce in potential effect of outages because of supporting data center outages. Any backup site used to store University Protected or Private data will include the same information security and privacy controls as the primary data center(s).

X. RIGHT TO AUDIT

Service Provider agrees that, as required by applicable state and federal law, auditors from state, federal, Florida State University, or other agencies so designated by the State or University, shall have the option to audit the outsourced service. Records pertaining to the service shall be made available to auditors and the University during normal working hours for this purpose.

Section B – Special Contract Requirements to meet Law, Regulation, or Contractual Obligations

Family Educational Rights and Privacy Act (FERPA) - Student Education Records

Institutions of higher education might have other obligations regarding use of data under federal, state, or local laws, regulations, or contractual obligations. Generally speaking, an institution may not be able to alleviate such obligations by contracting with a third party to perform functions that use regulated data. Clauses that include instructions to contracting third parties regarding regulatory requirements help to protect the institution in the event of an unauthorized disclosure or breach. The

Family Educational Rights and Privacy Act (FERPA) provides specific protections for student education records. In situations where confidential student data is hosted or accessed by a Service Provider, the contract with the Service Provider must acknowledge and address FERPA protections and obligations.

Sample Contract Clauses:

1. The [Service Provider] acknowledges that certain information about the Institution's students is contained in records; maintained by the [Service Provider] and that this information can be confidential by reason of the Family and Educational Rights and Privacy Act of 1974 (20 U.S. C. 1232g) and related Institution policies unless valid consent is obtained from the University's students or their legal guardians. Both parties agree to protect these records in accordance with FERPA and Institution policy. To the extent permitted by law, nothing contained herein shall be construed as precluding either party from releasing such information to the other so that each can perform its respective responsibilities. The Institution shall advise Service Provider whenever any Institution students have provided consent to release information to an extent broader than as provided for by FERPA or Institution policy.
2. Service Provider agrees that it may create, receive from or on behalf of Institution, or have access to, records or record systems that are subject to the Family Educational Rights and Privacy Act ("FERPA"), 20 U.S.C. Section 1232g (collectively, the "FERPA Records"). [Service Provider] represents, warrants, and agrees that it will: (1) hold the FERPA Records in strict confidence and will not use or disclose the FERPA Records except as (a) permitted or required by this Agreement, (b) required by law, or (c) otherwise authorized by Institution in writing; (2) safeguard the FERPA Records according to commercially reasonable administrative, physical and technical standards that are no less rigorous than the standards by which [Service Provider] protects its own confidential information; and (3) continually monitor its operations and take any action necessary to assure that the FERPA Records are safeguarded in accordance with the terms of this Agreement. At the request of Institution, Service Provider agrees to provide Institution with a written summary of the procedures Service Provider uses to safeguard the FERPA Records.

US Health Insurance Portability and Accountability Act (*HIPAA*)-Covered Entity Protected Health Information (PHI) & Business Associate Agreement

Refer to the current HIPAA legislation to ensure compliance with current safeguarding rules when contracting to transmit HIPAA protected information to a third-party Service Provider. Those campus units designated as covered entities will need to engage the Service Provider in a Business Associates Agreement when transferring PHI outside of the University.

Contracts involving student health information require FERPA contractual protections. Per U.S. Department of Health and Human Services and the U.S. Department of Education,

> *When a school provides health care to students in the normal course of business, such as through its health clinic, it is also a 'health care provider' as defined by HIPAA. If a school also conducts any covered transactions electronically in connection with that health care, it is then a*

covered entity under HIPAA. As a covered entity, the school must comply with the HIPAA Administrative Simplification Rules for Transactions and Code Sets and Identifiers with respect to its transactions. However, many schools, even those that are HIPAA covered entities, are not required to comply with the HIPAA Privacy Rule because the only health records maintained by the school are "education records" or "treatment records" of eligible students under FERPA, both of which are excluded from coverage under the HIPAA Privacy Rule. See the exception at paragraph (2)(i) and (2)(ii) to what is considered "protected health information" (PHI) at 45CFR§ 160.103. In addition, the exception for records covered by FERPA applies both to the HIPAA Privacy Rule, as well as to the HIPAA Security Rule, because the Security Rule applies to a subset of information covered by the Privacy Rule (i.e., electronic PHI).

(See http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/hipaaferpajointguide.pdf for further guidance)

Payment Card Industry – Data Security Standards (PCI DSS) – Credit Card Transactions

The outsourcing of credit card processing through the use of a Service Provider must meet the adherence to specifications as defined by the Payment Card Industry Data Security Standard (PCI DSS). Any agreement with a Service Provider must document the duties required to protect University related credit card processing as specified in PCI DSS Version 3.0 section 12.8 through 12.9 in the contract. In addition, University units should obtain documentation, such as a Report on Compliance, on each anniversary year of the contract to verify the PCI DSS compliance status of the "Service Provider."

Gramm Leach Bliley (GLB) ACT – Student Financial Records

Student financial information is protected by the Gramm Leach Bliley Safeguards Rule (16 C.F.R. § 314). The transfer of any protected information to a Service Provider in connection with a financial product or service requires the University ensure, by contract, that the Service Provider implements and maintains appropriate safeguards for Customer Information.

The contract provisions should ensure the Service Provider agrees to implement and maintain a written comprehensive information security program containing administrative, technical and physical safeguards for the security and protection of University information and further containing each of the elements set forth in §314.4 of the Gramm Leach Bliley Standards for Safeguarding Customer Information (16 C.F.R. §314).