

EDUCAUSE Center for Applied Research

Research Bulletin

Volume 2009, Issue 22

**November 3, 2009**

# Privacy and Confidentiality: Holding Service Providers Accountable

Nadine Stern, The College of New Jersey



## Overview

You can't shake hands with a clenched fist.

—Indira Gandhi

Like many senior-most information technology (IT) leaders in higher education, I wear two hats. At The College of New Jersey (TCNJ) I serve as Vice President, Information Technology and Enrollment Services. At TCNJ, enrollment services includes records and registration, financial aid, and student accounts. In this dual role I am keenly aware of the connection between IT efforts to secure and protect confidentiality in enterprise-wide and departmental information systems and the protections specified in a variety of regulations for the privacy of nonpublic personal information.

College and university leaders have always faced tough decisions, and those decisions get even tougher when diminished resources curb our flexibility. There is a growing literature about the advantages—and risks—of outsourcing information systems that have become costly to self-operate. The influence of alternative sourcing strategies on higher education, including software as a service [SaaS] and cloud computing, points to a sticky dilemma: As stewards of personal and confidential information related to students, faculty, institutional staff, alumni, trustees, and other members of our institution's community, how can our institutional leaders make appropriate choices about outsourcing information systems to service providers while concurrently ensuring protection of the confidential, personal information? With vast stores of academic, research, personal, administrative, student, and health records to protect, how do we ensure that our contracts haven't omitted an important clause with respect to privacy and confidentiality?

In a very real sense, the cost of a confidentiality breach defies measurement. Not only does failure to adequately protect privacy have tremendous consequences for individuals whose confidentiality has been compromised, but it can cause irreparable, long-term damage to the assets and reputation of the institution. As we know, choosing to self-operate our information systems, such as student e-mail, can be "expensive" if a comparable service can be delivered at little or no cost by an external service provider. If we choose to self-operate because we distrust service providers to maintain confidentiality, there is a high cost to that distrust. How can institutional leaders make fully responsible decisions when so much is at stake? How can we structure contracts to protect confidentiality, facilitate fiscally responsible decisions, enable superior service from providers, and allow everyone involved to shake hands with shared commitments?

It was against this backdrop that I was prompted to respond to a posting on the EDUCAUSE CIO listserv in early August 2009. The posting came from a college that was considering engaging a consulting firm to redesign its public (Internet) and private (intranet) websites. The writer requested samples of contract language that addresses the confidentiality of college data and the contractor's responsibility in upholding the confidentiality. Coincidentally, spurred by the December 9, 2008, release of the Family Educational Rights and Privacy Act (FERPA) Final Rules, TCNJ had just completed a seven-month exercise to update contract language to address precisely this concern. I

offered to share our work with other colleges and universities. As a result, I was invited by the EDUCAUSE Center for Applied Research (ECAR) to participate in an interview that would lead to sharing our work more broadly through this research bulletin. Drawing on the TCNJ experience, this bulletin addresses the data privacy issues that must be covered by contractual language when entering into an agreement for externally provided IT services or for external consulting about institutional systems. It covers instances in which external agents have access to data that is considered confidential and/or where data can be linked to personally identifiable records. It is based on work done at TCNJ between November 2008 and May 2009.

## Highlights of Holding Service Providers Accountable for Confidentiality

### **ECAR: What prompted TCNJ to develop the contract language in its *Service Provider Requirements* document?**

**Nadine Stern:** The issues of confidentiality and privacy related to student records are of paramount importance in higher education. As stewards of these records, TCNJ departments (including IT) are accountable for safeguarding the records covered by FERPA. We are obligated both to our students and to our institution to abide by the FERPA Final Rules. It seems to me that the topic of appropriate language for institutional contracts ought to be very hot at colleges and universities, not only when we consider outsourced service but also when we engage consultants to work with us on our information systems. Writing the right contract for outsourcing or consulting is a big concern, and we must be vigilant and disciplined in this effort. TCNJ has been working with a trusted IT consulting partner for many years, and issues related to confidentiality and privacy were tacitly understood and honored. When the FERPA Final Rules were issued in December 2008, we revisited the language in our contract with this consulting partner to examine how these contracts complied with the important FERPA regulations regarding protection of personal information, confidentiality, and nondisclosure. We realized that our contracts fell short of specifying service provider responsibilities in these domains according to the Final Rules, so we began a campus-wide process to address these shortcomings.

### **ECAR: When, and over what period of time, was the *Service Provider Requirements* document developed?**

**Stern:** I went back through my records to check on this, since it seemed like a very long process. In fact, it took about seven months. My first e-mail on this topic was sent in November 2008, and we completed the TCNJ *Service Provider Requirements* in May 2009. When I realized that we needed to review our contract language, it occurred to me that a good way to start was to ask our current consulting firm's account executives if they had contracts with other organizations that included language that covered FERPA requirements. Interestingly, they did not, and the account executives said that over the many years in which they had been working with higher education institutions, they had never been asked about this. Nonetheless, they were eager to become a test case for developing a template that would address the FERPA Final Rules in all TCNJ contracts.

The provider fully participated in the process of having the language reviewed and approved by legal counsel (both theirs and ours) and by other appropriate individuals as well. The cooperation they offered and delivered was not only appreciated, but it helped steer us all in the right direction. We hope they will also now benefit by being able to share this with other higher education clients.

**ECAR: What barriers had to be overcome in order to create the *Requirements*?**

**Stern:** Although it did not turn out to be much of a barrier in the end, our first challenge was to explain to our service provider why we needed to develop the *Requirements*. We had to clarify what we were asking for. At first, there was some reluctance to engage because it wasn't clear to the provider where this request was coming from, but once it became clear that we were asking the provider to participate because it was already a trusted partner, the path was cleared. Our second barrier was what I call "legalese." Contracts are difficult to write because the language must be as unambiguous as possible. Fortunately, contract attorneys are sticklers for precision. For example, there is a distinction between "confidential data" and "personally identifiable information." When we drafted the *Service Provider Requirements*, we had to decide when we needed to stick with those terms and when we could use a term such as "personal information" to say what we meant. During our process, we also discovered that much of the language used in the early drafts of the *Service Provider Requirements* was actually covered in other documents, so we wound up removing that language. Between requests for proposals, purchasing agreements, consulting contracts, and a myriad of other institutional papers, there is quite a "package" of documents that needs to be considered when creating or updating one piece. I would characterize this challenge as "finding the right middle ground" and "considering the vendor package" for our *Requirements*.

**ECAR: Who was involved in developing the TCNJ *Service Provider Requirements*?**

**Stern:** You are asking who was on the bus, and whether we had the right people, right? The answer is simple: We had most of the right people, and if we had to do this again, I'd add some more. From the TCNJ side we included General Counsel and me (VP for IT and Enrollment Services). Had it not been for the fact that I serve both IT and Enrollment Services, we would have included someone from the registrar's office. From the service providers we included our account executives and their legal counsel. In retrospect, we should definitely have included the TCNJ Associate Treasurer, who handles all purchasing regulations and contracts. He would have contributed tremendous value to our process and would have saved us all a lot of time. We shall remember to include him the next time around!

**ECAR: In what circumstances, and under what conditions, do you anticipate making use of the *Requirements*?**

**Stern:** We will use the template *Requirements* document for any consulting engagement where an outside firm works with confidential TCNJ data. We are currently considering outsourcing possibilities, such as student e-mail and services offered as software as a service or in the cloud. Where it is appropriate, we will apply these *Requirements* in

contracts related to private information. Because the FERPA rules have been updated, we're taking this opportunity to do campus-wide training about what people can and can't do under FERPA. Interestingly, there are widespread misunderstandings about what an education record really is, and who can discuss what with whom. We hope these training sessions will clear up these misunderstandings.

**ECAR: What circumstances will this *Requirements* document not cover, and why?**

**Stern:** *Service Provider Requirements* might serve as a foundation for contracts related to other regulations such as Gramm-Leach-Bliley, but it might be insufficient to cover the myriad confidentiality issues related to personal health information addressed by the Health Insurance Portability and Accountability Act (HIPAA). We plan to apply these *Requirements* in a carefully examined way for each contract that is drawn up and adapt it as needed.

**ECAR: What external resources did you use, if any, to provide insights or language suggestions for this *Requirements* agreement?**

**Stern:** As always, we are grateful to many individuals in the higher education community for their insights, inspiration, information, help, and support through this important process. One of the resources we relied heavily on was Rodney Petersen, the EDUCAUSE Government Relations Officer and Director of EDUCAUSE Cybersecurity Initiative. On behalf of EDUCAUSE and its college and university membership, Rodney kept us all posted on the progress of the FERPA Final Rules deliberations and, most importantly, on the implications for our campuses. We also benefitted greatly from a webinar organized by John Snodgrass of Chapman University. John had been registrar at Chapman for nine years until March 2009, when he became associate vice chancellor of student services online for Chapman University College [which has since become Brandman University].

**ECAR: What kind of resources did you wish were available as you produced the *Requirements*? What could/should the higher education community or EDUCAUSE provide as a shared resource to help standardize agreement documents like this?**

**Stern:** I wish I had been able to easily find a template for a sample *Service Provider Requirements*. I understand that some have been published [see the "Where to Learn More" section for citations from the Catholic University of America and EDUCAUSE/Internet2], but I was not able to easily find them. I would certainly have used a template as a starting point, and seeing language that had been vetted through the higher education community would have instilled confidence that we were including all of the important considerations in our *Requirements*. Discussions on the CIO listserv indicated that other institutions agree that a template for contract language would be helpful.

**ECAR: Are you willing to have the TCNJ *Service Provider Requirements* document referenced online or published as part of this research bulletin, assuming there is space and it is appropriate to do so?**

**Stern:** Absolutely! We are eager to share our work with others who might benefit from it. The TCNJ *Service Provider Requirements* document is available on the web at [http://www.tcnj.edu/~it/procedures/documents/TCNJ\\_SP\\_REQ.pdf](http://www.tcnj.edu/~it/procedures/documents/TCNJ_SP_REQ.pdf). [The text of the *Service Provider Requirements* document is also included in the Appendix to this research bulletin, starting on page 8.]

## What It Means to Higher Education

### **ECAR: What are the most important things to share with others in higher education about the importance of having a requirements document?**

**Stern:** First, in order to fully comply with federal, state, institutional, and other regulations, it is absolutely necessary to examine contract language for the protection of our students and the university community as a whole. Second, the changing nature of the IT services we will all be using (i.e., consulting, outsourcing, SaaS, and so forth) makes it imperative that our institutions do everything necessary to protect the identities and preserve confidentiality for the people who entrust us with confidential information. Third, identity theft is becoming an ever greater problem, and, as many of us have experienced personally, the consequences are dire. Perhaps as a result of these very high stakes, the world seems to have become more litigious. For all of these reasons, we need to be more vigilant than ever about ensuring that organizations that have access to confidential records behave fully responsibly.

### **ECAR: What are the most important lessons you learned through the process of developing the TCNJ *Service Provider Requirements*?**

**Stern:** Lesson 1—Do this before you need it. Updating contracts and developing important, unambiguous language should not be done under the pressure of time. You don't want to have to engage important, busy people at your institution in a last-minute, rush project just because a wolf is knocking at your door. We all know that this needs to get done, so let's do it without urgency.

Lesson 2—Embed your service provider requirements into your initial contract negotiations. Let potential service providers know up front that, a) you are very serious about privacy and confidentiality protections, and, b) in order to win your confidence (and the contract), they must demonstrate how they will comply with the terms.

Lesson 3—Include your legal and purchasing departments in the initial and ongoing discussions about contracts.

### **ECAR: What would you do differently next time?**

**Stern:** I would have started the process much earlier. In essence, we had to construct an "after-the-fact" set of requirements, but these requirements should really have been an integral part of the purchasing process. I am currently working with the TCNJ General Counsel to make sure that these requirements become standard for vendors that wish to work with TCNJ. It is possible that other institutions are way ahead of us in terms of having appropriate language in their standard purchasing material, but I suspect some

IT leaders will want to verify whether the issues covered in our *Service Provider Requirements* are, in fact, addressed at their institutions.

**ECAR: What else would you like to tell readers of this ECAR research bulletin?**

**Stern:** Don't be afraid to ask other institutions for samples of their work. We all have plenty to keep us busy—there is no need to reinvent this wheel at each institution. Regulations such as FERPA have a common impact across higher education, regardless of institution size, governance, or Carnegie Class. This is a great opportunity for our community to share and benefit from the wisdom of the crowd.

## Key Questions to Ask

- How does our institution protect the privacy of members of the university community and the confidentiality of education records and institutional assets when granting access to this information to agencies or individuals external to the institution?
- To what degree do the purchasing and contractual agreements on behalf of our institution specify requirements keeping nonpublic personal information confidential?
- Do our contracts conform to the FERPA Final Rules issued in December 2008?
- As regulations change, what programs do we have in place to ensure that individuals on campus who deal with FERPA regulations are kept up-to-date on what the rules are and how they should be applied?

## Where to Learn More

- Catholic University of America, “Data Security Terms for Inclusion in Contracts with Service Providers,” January 21, 2009, <http://counsel.cua.edu/FERPA/resources/contract.doc>.
- The College of New Jersey, *Service Provider Requirements*, August 2009, [http://www.tcnj.edu/~it/procedures/documents/TCNJ\\_SP\\_REQ.pdf](http://www.tcnj.edu/~it/procedures/documents/TCNJ_SP_REQ.pdf).
- EDUCAUSE/Internet2 Security Task Force Data Protection Contractual Language, <https://wiki.internet2.edu/confluence/display/itsg2/Data+Protection+Contractual+Language>.
- U.S. Department of Education, 34 CFR Part 99, “Family Education Rights and Privacy; *Final Rule*,” Federal Register 73, No. 237, December 9, 2008. <http://edocket.access.gpo.gov/2008/pdf/E8-28864.pdf>.

# Appendix: Service Provider Requirements

## The College of New Jersey

### SERVICE PROVIDER REQUIREMENTS

Pursuant to the Agreement, Company XXX ("Service Provider") is a service provider to whom The College of New Jersey ("TCNJ") shall provide access to customer (including student) nonpublic personal information. Service Provider shall provide adequate safeguards for the protection of the confidentiality of such information. To the extent applicable to the performance of Service Provider under the Agreement, those safeguards shall conform to the requirements of the Family Educational Rights and Privacy Act ("FERPA")<sup>1</sup> and its implementing regulations,<sup>2</sup> the Gramm-Leach-Bliley Act<sup>3</sup> ("GLBA"), the Federal Trade Commission's *Standards for Safeguarding Customer Information*<sup>4</sup> (the "Safeguards Rule") and the Fair and Accurate Credit Transactions Act of 2003<sup>5</sup> ("FACTA") (which amends the Fair Credit Reporting Act<sup>6</sup> ("FCRA")) and regulations issued by the Federal Trade Commission ("FTC"), the federal bank regulatory agencies, and the National Credit Union Administration ("NCUA") (the "Red Flag Rules")<sup>7</sup> requiring financial institutions and creditors to develop and implement written identity theft prevention programs (collectively, these statutes and regulations may be referred to as the "Privacy Laws"). The confidentiality, security and other requirements set forth in this Exhibit (the "Service Provider Requirements") shall comprise the minimum safeguards to be employed by Service Provider.

#### 1. Definitions

- 1.1. "Personal Information" means any confidential and proprietary information and documents, (including education records under FERPA, and nonpublic personal information), in any form (e.g., electronic, paper, or other) concerning any TCNJ Community Members that are submitted under this Agreement or which Service Provider becomes aware of during the course of its performance hereunder.
- 1.2. "Nonpublic personal information" takes the meaning provided in the FTC's *Privacy of Consumer Financial Information Final Rule*<sup>8</sup> (the "Privacy Rule"), except that in this context nonpublic personal information is not limited to information about customers or consumers of TCNJ that seek or are provided financial products or services, but rather nonpublic personal information includes information about TCNJ Community Members regardless of whether they seek or obtain any financial product or service. Examples of nonpublic personal information include the following: TCNJ Community Member's social security number, address, grades, employment data and any other personally identifiable information that if disclosed without authorization might result in substantial harm or inconvenience or liability under applicable privacy laws.
- 1.3. "TCNJ Community Members" means current or former or prospective trustees, officers, faculty, staff, employees, students, volunteers, agents, or representatives of TCNJ or its affiliates.

## 2. Personal Information Confidentiality and Nondisclosure

Personal Information shall be considered property of TCNJ. Service Provider shall hold all Personal Information in the strictest confidence and in accordance with applicable laws and regulations as well as TCNJ's policies and procedures. Service Provider shall obtain no proprietary rights (directly or indirectly) in or to the Personal Information. Service Provider shall not disclose the Personal Information to any third party without the prior written consent of TCNJ unless (i) required to perform Service Provider's obligations under the Agreement or (ii) required by law in which event Service Provider shall promptly notify TCNJ of such request or requirement. Service Provider shall use such Personal Information only in connection with the furtherance of the business relationship between the parties, and Service Provider shall make no further use, in whole or in part, of any such Personal Information. Service Provider further agrees to disclose the Personal Information only to its employees whose services are required in furtherance of the objectives of the business relationship between the parties, and to require each of its employees to comply with the terms of this Agreement, prior to the disclosure to such employees. Upon the expiration or termination of this Agreement, for any reason, Service Provider shall promptly turn over and return to TCNJ all Personal Information (in whatever form or media) or upon the written direction of TCNJ, destroy the Personal Information.

## 3. Service Provider Safeguards Statement

Service Provider has submitted a statement (the "Service Provider Safeguards Statement," a copy of which is attached hereto) to TCNJ that defines what steps Service Provider is taking and shall take to protect TCNJ customer information. Service Provider shall review the Service Provider Safeguards Statement and revise as appropriate not less than annually. Service Provider shall comply with the requirements included in the Service Provider Safeguards Statement. TCNJ may annually (or more frequently as circumstances require in TCNJ's judgment) conduct a review, in connection with the Agreement, of Service Provider's compliance with the Service Provider Safeguards Statement, Service Provider Requirements, and the Privacy Laws.

## 4. Service Provider Agreements, Acknowledgments, Representations and Warranties

Service Provider agrees, acknowledges, represents and warrants as follows:

- 4.1. The Agreement permits Service Provider access to Personal Information, including, without limitation, nonpublic personal information such as:

Personally identifiable student record information and a broader range of other personally identifiable, non-public, student and/or employee information.

- 4.2. Service Provider shall hold the Personal Information in strict confidence and access it only for the explicit business purpose of the Agreement.

- 4.3. Service Provider shall ensure compliance with the confidentiality and security conditions of the Agreement, Service Provider Safeguards Statement and Service Provider Requirements and, as applicable, the Privacy Laws.
- 4.4. Service Provider shall protect the Personal Information it accesses according to commercially acceptable standards and no less rigorously than it protects its own and its customers' confidential information.
- 4.5. TCNJ may require the prompt return or destruction of all copies of Personal Information received by Service Provider upon completion of the Agreement.
- 4.6. Service Provider stipulates to allowing the entry of injunctive relief without the posting of bond in order to prevent or remedy breach of the confidentiality obligations of the Agreement.
- 4.7. Service Provider stipulates that any violation of the Service Provider Requirements shall constitute a material breach of the Agreement and entitles TCNJ to immediately terminate the Agreement without penalty to TCNJ.
- 4.8. Service Provider shall maintain controls to ensure that any subservicer used by Service Provider will also be able to protect and will protect customer information.
- 4.9. TCNJ may request copies of audits and test result information that indicate the degree to which Service Provider and any subservicers implement appropriate information security measures in connection with the Agreement.
- 4.10. TCNJ may audit Service Provider's compliance with Service Provider Requirements and Service Provider shall cooperate with TCNJ in any such audits.
- 4.11. Service Provider Requirements shall survive any termination of the Agreement.

- 
1. U.S. Department of Education, Family Education Rights and Privacy Act (FERPA), U.S. Code Title 20, Chapter 31, Subchapter III, Part 4, § 1232g (20 U.S.C. § 1232g), <http://www.ed.gov/policy/gen/guid/fpc/ferpa/index.html>.
  2. U.S. Department of Education, Family Education Rights and Privacy Act (FERPA), 34 CFR Part 99, <http://www.ed.gov/policy/gen/reg/ferpa/index.html>.
  3. Gramm-Leach-Bliley Act, Disclosure of Nonpublic Personal Information, Pub. L. 106-102 (1999), 15 U.S.C. §6801 *et seq.*, <http://www.ftc.gov/privacy/qlbact/qlbsub1.htm>.
  4. Federal Register, Federal Trade Commission, 16 CFR Part 314, Standards for Safeguarding Customer Information; Final Rule, <http://www.ftc.gov/os/2002/05/67fr36585.pdf>.
  5. Fair and Accurate Credit Transactions Act of 2003, Pub. L. 108-159, [http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108\\_cong\\_public\\_laws&docid=f:publ159.108](http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ159.108).
  6. Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681 *et seq.*, <http://www.ftc.gov/os/statutes/031224fcra.pdf>.
  7. Federal Trade Commission, Identity Theft Rules, 16 C.F.R. Part 681.2, [http://www.nacubo.org/documents/business\\_topics/FTC%20Red%20Flags%20RULE.pdf](http://www.nacubo.org/documents/business_topics/FTC%20Red%20Flags%20RULE.pdf).
  8. Federal Register, 16 C.F.R. § 313, Privacy of Consumer Financial Information; Final Rule, May 24, 2000, <http://www.ftc.gov/os/2000/05/65fr33645.pdf>.

## About the Author

*Nadine Stern (stern@tcnj.edu) is Vice President, Information Technology and Enrollment Services, The College of New Jersey.*

## Copyright

Copyright 2009 EDUCAUSE and Nadine Stern. All rights reserved. This ECAR research bulletin is proprietary and intended for use only by subscribers. Reproduction, or distribution of ECAR research bulletins to those not formally affiliated with the subscribing organization, is strictly prohibited unless prior permission is granted by EDUCAUSE and the author.

## Citation for This Work

Stern, Nadine. "Privacy and Confidentiality: Holding IT Service Providers Accountable" (Research Bulletin, Issue 22). Boulder, CO: EDUCAUSE Center for Applied Research, 2009, available from <http://www.educause.edu/ecar>.