Key Issues in Contracting for Information Technology Resources and Services

May 18, 2011

The "Issue" section in this checklist was derived from materials presented at the 2009 conference of the National Association of College and University Attorneys (NACUA). The "Sample Language" sections were added by Texas State to serve as examples of contract language to address the issue. While these examples have been individually reviewed by the university's legal counsel, circumstances vary and sample provisions may not be appropriate in all situations. Additional legal review of the language in the context of the agreement is strongly recommended.

The following definitions apply to terms found in the sample language sections and may apply to different terms in any specific contracts under consideration:

Agreement:	the contract between the Vendor and the Institution
CDI:	Covered Data and Information, the institutional data and information is held by or accessible to the Vendor under the Agreement.
Constituent:	an institutional affiliate that uses the information system, component, or service (e.g., faculty, staff, students, retirees, alumni, etc.)
Institution:	the recipient of the information system, component, or service
Vendor:	the provider of the information system, component, or service including subcontractors

The Issues Checklist

[ ] Issue: FERPA (and privacy and confidentiality in general)

Much of our data – including student information databases and much faculty and staff e-mail – constitutes "education records" for purposes of FERPA and therefore may be outsourced only to vendors that we have designated, and that are willing to accept designation, as "school officials" with "legitimate educational interests" in the data. In order to do that, we must ensure both that our definitions of those two terms in our FERPA annual notices are broad enough to cover outsourcing and that the vendor will not use the data for any purpose other than providing the outsourced service (such as data mining for the vendor's own benefit) or disclose it to others without appropriate authorization.

There may be similar requirements under other statutes governing the privacy and confidentiality of specific types of information, and we are likely to want to protect the privacy and confidentiality of most of our data in any event. Any such requirements or desires should be set forth expressly in the contract, or they will not be enforceable. If the vendor is able to provide encryption of our data in both transmission and storage, privacy concerns, and the need for other contractual protections, may be lessened or even eliminated.

Sample Language:

"Vendor shall comply with all federal, state, and local privacy laws or regulations applicable to the CDI provided by Institution and its Constituents, including but not limited to: the Family Educational Rights and Privacy Act (FERPA) (Pub. L. No. 93-380 (1974), codified at 20 U.S.C. § 1232g); the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (Pub. L. No. 104-191, § 264 (1996), codified at 42 U.S.C. § 1320d; Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. § 160 (2002), 45 C.F.R. § 164 subparts A, E (2002)."

"Vendor agrees to hold CDI in strict confidence. Vendor shall not use or disclose CDI received from or on behalf of Institution or its Constituents except as permitted or required by the Agreement, as required by law, or as otherwise authorized in writing by Institution. Vendor agrees that it will protect the CDI it receives from or on behalf of Institution or its Constituents according to commercially acceptable standards and no less rigorously than it protects its own confidential information."

[ ] Issue: Data Security

If they address the issue at all, vendor form contracts are likely to promise to provide only "reasonable" security for your data, or perhaps to adhere to "industry standard" security practices. While such promises sound good in the abstract, they are open to considerable interpretation and argument. It is preferable to specify an actual, specific, independent security standard and require that it be updated, and perhaps

audited, regularly. In addition, for certain kinds of data (e.g., data subject to HIPAA, Gramm-Leach-Bliley, PCI-DSS, or the Massachusetts Standards for the Protection of Personal Information of Residents of the Commonwealth), there may be specific security requirements that must be included in any vendor contracts. Ideally, the contract should also provide for regular SAS 70, Type II audits, with customer access to the results.

Finally, the contract should require the vendor to give us notice of any security/data breaches, and, to the extent that user notification is legally required, such notice should preferably be in advance of user notification (which should be the vendor's responsibility).

Sample Language:
"Vendor shall develop, implement, maintain and use appropriate administrative, technical and physical security measures to preserve the confidentiality, integrity and availability of all electronically maintained or transmitted CDI received from or on behalf of Institution or its Constituents. These measures will be extended by contract to all subcontractors used by Vendor."

"Vendor shall provide Institution with access to its latest SAS 70 Type II audit results, Shared Assessments™ security questionnaire(s), or similar independent security assessment findings, or permit Institution to conduct its own assessment upon request once every two years."

"Vendor shall, within one day of discovery, report to Institution any use or disclosure of CDI not authorized by this Agreement or in writing by Institution. Vendor's report shall identify: (i) the nature of the unauthorized use or disclosure, (ii) the CDI used or disclosed, (iii) who made the unauthorized use or received the unauthorized disclosure, (iv) what Vendor has done or shall do to mitigate any deleterious effect of the unauthorized use or disclosure, and (v) what corrective action Vendor has taken or shall take to prevent future similar unauthorized use or disclosure. Vendor shall provide such other information, including a written report, as reasonably requested by Institution."

"In the event of a security breach within the Vendor's control and covered under the Texas Breach Notification Law (Texas Business and Commerce Code § 521.03), Vendor shall bear all responsibility and expense for complying with the disclosure and notification requirements under that statute."

"Vendor agrees to hold CDI in strict confidence. Vendor shall not use or disclose CDI received from or on behalf of Institution or its Constituents except as permitted or required by the Agreement, as required by law, or as otherwise authorized in writing by Institution. Vendor agrees that it will protect the CDI it receives from or on behalf of Institution or its Constituents according to commercially acceptable standards and no less rigorously than it protects its own confidential information."

[ ] Issue: Access to data for purposes of e-discovery

Although the contract probably will not (and probably need not) expressly address the issue, it is important to understand – ahead of time – the architecture of the vendor's system, how and in what format it keeps your data, and what tools are available to you to access your data, so that you will be ready for any e-discovery needs that may arise. "Free" services typically will have few such tools available, which likely will make e-discovery a time-consuming and cumbersome task.

Sample Language:
"Both the Vendor and Institution shall facilitate the lawful disclosure of CDI for e-discovery purposes, or pursuant to applicable state or federal laws, or by request or order of any court or government agency. Provided, however, before making such a disclosure of CDI, Vendor must give Institution and all affected Constituents prior written notice of that disclosure, which must identify: the CDI that Vendor intends to disclose, the law(s), request, or order under which Vendor believes it is required to make such a disclosure, the persons or entities to whom Vendor intends to disclose such CDI, and the date on which Vendor is required to make such a disclosure."

"Vendor shall make itself and its employees, subcontractors, or agents assisting Vendor in the performance of its obligations under the Agreement available to Institution at no cost to Institution to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings against Institution, its directors, officers, agents or employees based upon a claimed violation of laws arising out of this Agreement."

[ ] Issue: Location of data

Some vendor form contracts expressly reserve the right to store customer data in any country in which they do business. Others may not address the issue, but the vendors may follow similar practices nevertheless, on the (generally legitimate) theory that what is not expressly prohibited is thereby permitted. While dispersed geographical storage is beneficial from a data protection and backup perspective, it can raise export control (EAR/ITAR) issues in the context of research data. If that is important to you, you should be sure to include language prohibiting "extraterritorial" storage.

Sample Language:
"Vendor shall store and process all CDI subject to the legal jurisdiction of the United States of America, or under the concurrent jurisdiction of the Unites States of America and one or more of its states, and free from any foreign legal jurisdiction at all times."

[ ] Issue: Ownership of data

The contract should expressly make clear that all data belongs to the institution (and/or its users) and that the vendor acquires no rights or licenses, including without limitation intellectual property rights or licenses, to use the data for its own purposes by virtue of the transaction. It also may be useful to provide that the vendor does not acquire and may not claim any security interest in your data.

Sample Language:
"Vendor acknowledges that the Agreement allows the Vendor access to CDI provided by Institution and its Constituents, that all such CDI remains the intellectual property of the providing party and that Vendor acquires no rights or licenses to use CDI for any purpose not expressly authorized in the Agreement."

[ ] Issue: Unauthorized or inappropriate use

Vendor form contracts may attempt to make us responsible for affirmatively preventing any "unauthorized" or "inappropriate" use of the vendor's service by others, or perhaps to use "best efforts" or "commercially reasonable efforts" to do so. Given that these services are "in the cloud" and therefore largely outside our control, it is preferable to provide only that we will not "authorize" or "knowingly allow" such uses.

Such contracts also may require us to notify the vendor of "all" unauthorized or inappropriate uses of which we become aware. Particularly with respect to vendors with broadly stated AUPs or terms of service, such expansive obligations seem burdensome and unnecessary. It is preferable to replace "all" with "material" or some similar, higher threshold.

Sample Language:
"Institution does not monitor the use of Vendor's services by Institution's Constituents. Institution will not authorize or knowingly permit unacceptable use of Vendor services by Institution's Constituents and will notify Vendor of any material violations of Vendor policies, terms of service, or similar provisions by Institution's Constituents."

[ ] Issue: Suspension of end user accounts

E-mail services in particular may wish to retain the right to suspend your end users for violations of the vendor's AUP or terms of service. If, as is common, those provisions are broadly stated, the vendor will have almost open-ended authority to suspend your users. It is preferable to limit any such power to a more restrictive standard – perhaps only "material" violations, or violations that "significantly" threaten the security or integrity of the vendor's system.

Sample Language:
"Vendor shall not normally suspend or otherwise disrupt the use of Vendor's services by one or more Constituents without prior notice to Institution and affected Constituents. Vendor may suspend or disrupt a Constituent use of Vendor services without notice if such use constitutes a material and significant threat to the confidentiality, integrity, performance, or availability of the Vendor's systems or services."

[ ] Issue: Emergency security issues

Vendors understandably may wish to have the right to "immediately" suspend an "offending use," and possibly the service altogether, in the event of an "emergency" issue. However, the standard for what constitutes an emergency should be clearly defined, should not give the vendor much if any discretion or flexibility in its application, and, preferably, should incorporate a "materiality" or similar threshold.

Sample Language:
Same as for "Suspension of end user accounts".

[ ] Issue: Suspension and termination of the service

Vendor form contracts typically give the vendor the right to suspend the service or to terminate it altogether upon certain events or conditions. Such provisions are not unreasonable in the abstract, but they should be limited in scope to only truly significant matters, provide for an opportunity for you to cure the alleged violations or some form of escalation rather than instantaneous implementation (except in the case of true emergencies), and give you adequate time to make alternative arrangements for your data or service. (In the case of an e-mail system, it may take 6 months or more to establish and transition to a new system, particularly if you intend to completely dismantle your internal system once you outsource.) It also will be important to have assurance your data will continue to be available to you, in a usable format, for at least that long (or, if the vendor is unwilling to commit to a specific length, a "commercially reasonable" period of time) following any termination, as well as that the vendor will return or destroy any copies of your data once transition is complete.

Sample Language:
"Should Vendor wish to terminate this Agreement for cause prior to its normal expiration, Vendor shall (i) first provide Institution with at least NN days to cure the violation in question; (ii) allow Institution NN business days to find or develop a suitable replacement for Vendor's service; (iii) sustain Institutional and Constituent access to Institution's CDI while transitioning to a replacement service; and (iv) return or destroy all copies of Institution's CDI following the transition to a replacement service."

[ ] Issue: Service level agreements

The amount of guaranteed "uptime," the process and timeline for dealing with "downtime," and the consequences for any failures to meet those requirements should be spelled out clearly. In the context of a "free" service, additional "free" service is of no great benefit to us, and no great disincentive to the vendor.

Sample Language:
The language for this issue will be highly dependent upon the specific service and institutional situation.

[ ] Issue: Disclaimer of warranty

Vendor form contracts typically disclaim essentially all warranties, sometimes expressly including any warranty that the vendor's service does not infringe third-party intellectual property rights. At a minimum, the contract should warrant that the service conforms to and will perform in accordance with its specifications (which should themselves be as detailed as possible, to avoid misunderstandings and disagreements) and that it does *not* infringe any third-party intellectual property rights. Without those two warranties, there is no enforceable assurance that the service will in fact do what the vendor's marketing people claim it will do or that the vendor even has the right to provide it to us – and, if it doesn't work, or if we are sued for infringement, we will have no recourse against the vendor.

Sample Language:
"Vendor acknowledges that the Agreement allows the Vendor access to CDI provided by Institution and its Constituents, that all such CDI remains the intellectual property of the providing party and that Vendor acquires no rights or licenses to use CDI for any purpose not expressly authorized in the Agreement."

[ ] Issue: Indemnification by customer

Some vendor form contracts require us to indemnify the vendor not only for our own actions (which is not necessarily unreasonable), but also those of our end users, including students for whom we are not otherwise vicariously liable. With respect to liability for student e-mail, online postings, and the like, this is largely an issue of who will pay the vendor's attorney fees, as the vendor has good legal defenses against claims based on end user content or actions. Moreover, this is not really taking on a new liability, as we currently can be sued for such content or actions (and have the same legal defenses) as ISPs ourselves. Nevertheless, it is preferable not to voluntarily accept that liability, which is also no different that the vendor's liability for any other, non-institutional end users.

Public institutions may also have significant state-law restrictions on their ability to indemnify.

Sample Language:
"Institution is a Texas state agency and its indemnity obligations in this Agreement apply only to the extent permitted by Texas law. Institution's liability is limited by sovereign immunity and laws such as the Texas Tort Claims Act. Institution does not waive any of its rights or defenses under Texas law."

[ ] Issue: Indemnification by vendor

Vendor form contracts rarely include any form of indemnification benefitting us, but such protection is critical in at least two areas: infringement of third-party intellectual property rights and inappropriate disclosure or data breach, both of which are largely, if not entirely, in the vendor's sole control, and both of which can be extremely costly to defend and remedy. (If, as has happened, a vendor refuses to accept liability for either of these issues on the ground that it's a "black hole," we should take that as a great warning about the vendor's lack of confidence in its own service and look elsewhere – what the vendor is really saying is that it expects *us* to be its insurance company.) Ideally, the vendor would indemnify us for all of its acts and omissions.

Sample Language:
"Vendor shall defend and hold Institution harmless from all claims, liabilities, damages, or judgments involving a third party, including Texas State's costs and attorney fees, which arise as a result of Vendor's acts, omissions, or failures to meet any of its obligations under this Agreement."

[ ] Issue: Modifications to the contract

Vendor form contracts sometimes reserve the right for the vendor to make modifications to its services unilaterally. While some form of right to make changes probably is necessary and appropriate – we certainly would have no objection to improvements – such language is overbroad and does not provide the customer with any assurance that any such modifications will be beneficial, let alone acceptable. Limiting the vendor's right to "commercially reasonable modifications" would be an improvement, but, in the context of a "free" service, could still be expansive. Even better would be to add to that a qualification prohibiting "materially detrimental" modifications."

Sample Language:
"Vendor may make commercially reasonable modifications to the Service without prior notice to Institution, provided that such modifications do not materially diminish the nature, scope, or quality of the Vendor's Service."

[ ] Issue: Incorporation of URL terms

Similarly, vendor form contracts may incorporate by reference additional terms and policies posted to the vendor's web site, which typically are subject to the vendor's unilateral amendment, and those terms and policies may in turn incorporate by reference still other terms and policies posted elsewhere on the vendor's

web sites, which also typically are subject to the vendor's unilateral amendment. The result is that the contract itself is incomplete, it may well contain provisions that are inconsistent or that conflict with the incorporated provisions, and it likely will be difficult or impossible to fully comprehend. It also will potentially be meaningless, because the vendor will have the right to amend it significantly at any time, and likely even without any more notice to us than posting the change to its web site. While it may be reasonable to deal with technical standards and guidelines or other "non-legal" matters elsewhere, it is strongly preferable that all contractual terms be included in the contract itself. At the very least, the customer should attempt to require the vendor to provide direct, individual notice sufficiently in advance of the effective date of any amendments to incorporated terms, along with the right to terminate if such amendments are unacceptable or materially detrimental to the customer's interests.

Sample Language:
"Vendor expressly affirms that all applicable terms, conditions, and policies are contained within this Agreement and that the Agreement does not incorporate by reference any terms, conditions, or policies residing on Vendor's website or in any form external to this Agreement."

"Vendor shall provide a minimum of NN days advance notice to Institution prior to the effective date of any amendments to the terms, conditions, or policies incorporated by reference into this Agreement, including those terms, conditions, or policies residing on Vendor's website or in any form external to this Agreement. Institution reserves the right to terminate the Agreement without penalty if such amendments are unacceptable or materially detrimental to Institution's interest."

[ ] Issue: Governing law, jurisdiction

Almost certainly, a vendor's form contract will specify that it is governed by the law of the vendor's home state and grant the courts of that state exclusive jurisdiction over any disputes arising out of the contract. Public institutions generally have significant state-law restrictions on their ability to consent to such provisions, and they are inadvisable for others. It is preferable to either (a) specify the law and jurisdiction of our own state (large vendors likely operate in and are subject to all such jurisdictions, so it is no significant inconvenience for them), (b) provide that disputes must be brought in the defendant's jurisdiction (which is even-handed and tends to encourage informal resolution, as the plaintiff won't have the "home court" advantage), or (c) simply delete the provision and leave the question open for later argument and resolution if and when needed.

Sample Language:
"Agreement shall be governed and construed in accordance with the laws of the state of Texas. Unless otherwise mutually agreed, venue for all dispute resolution actions shall be in XXXXXXXXX County, Texas."

"Institution and Vendor agree that if either party initiates litigation or dispute resolution procedures based on this Agreement, it must do so exclusively in the jurisdiction of the defendant and under the laws of that jurisdiction."

[ ] Issue: Dispute resolution

Vendor's form contracts often specify the manner of dispute resolution in addition to the location. The form contract may attempt to limit or restrict the customer's legal options (e.g., a proscribed mediation program) in the event of a dispute. Public institutions are generally prohibited from accepting such conditions.

Sample Language:
"To the extent that Chapter 2260, Texas Government Code, applies to the Agreement and is not preempted by other applicable law, the dispute resolution process provided for in Chapter 2260 and the related rules adopted by the Texas Attorney General pursuant to Chapter 2260, will be used by Institution and Vendor to attempt to resolve any claim for breach of contract made by Vendor that cannot be resolved in the ordinary course of business, The parties specifically agree that (i) neither the execution of the Agreement by Institution nor any other conduct, action or inaction of any representative of Institution relating to the

Agreement constitutes or is intended to constitute a waiver of Institution's or the state's sovereign immunity to suit; and (ii) Institution has not waived its right to seek redress in the courts."

[ ] Issue: Access by individuals with disabilities

Texas Administrative Code §206 and Texas Administrative Code §213 establish accessibility standards for information resources deployed by Texas Institutions of Higher Education. TAC §213.38(b)(1) specifically states that: "Unless an exception is approved by the president or chancellor of an institution of higher education pursuant to §2054.460, Texas Government Code, and §213.37 of this chapter, or unless an exemption is approved by the department, pursuant to §2054.460, Texas Government Code, and §213.37 of this chapter, all electronic and information resources products developed, procured or changed through a procured services contract, and all electronic and information resource services provided through hosted or managed services contracts, shall comply with the provisions of Chapter 206 and Chapter 213 of this title, as applicable."

Sample Language:

"Vendor represents and warrants the electronic and information resources and all associated information, documentation, and support that Vendor provides to Institution under the Agreement comply with the applicable requirements set forth in Title 1, Chapters 206 and 213 of the Texas Administrative Code dealing with accessibility by individuals with disabilities (as authorized by Chapter 2054, Subchapter M of the Texas Government Code)."