UNC CHARLOTTE

The Science of the Deal: Negotiating Technology Terms in Contracts

Amy S. Kelso, Senior Associate General Counsel

Fall 2016 Legal Symposium

September 29, 2016

UNC CHARLOTTE

What We'll Cover

- Is this just another contract checklist training?
- What are some typical technology issues in contracts?
- What do I need to look for?
- What do I add/delete?
- What University standards/guidelines/policies/resources are available?

UNC CHARLOTTE

Let's Review the Contract Checklist

Is this another contract checklist training? ("groan")

NO, but let's review the bare-bones basics…

https://legal.uncc.edu/legal-topics/contracts/contract-checklist

- contract
- agreement
- memorandum of understanding (MOU)
- affiliation
- grant
- lease/license
- release
- any time the university is agreeing to do something (including making payment) in exchange for another party's action, product, or service

UNC CHARLOTTE

A Few No-Nos

- Governing law/jurisdiction: has to be NC (or delete!)
- Indemnification: We can't agree to indemnify--look out for these words:
  - "indemnify"
  - "hold harmless"
  - "defend"
  - "release"
  - "waive"
- Attorneys' fees/court costs
- Arbitration--cannot be binding
- Non-compete clause
- Liquidated damages
- Assignment of rights
- NC Statute of Limitations = 3 years

UNC CHARLOTTE

Technology in Contracts

That's all old news, but what about technology contracts?

- What kinds of contracts are we talking about?
- What kinds of issues do I look for?
- What do I add?
- What do I delete?
- Where can I find more info?

UNC CHARLOTTE

What Kinds of Contracts?

Contracts with vendors for services, software, hardware, or subscriptions, such as…

- External hosting/processing/transmission/storage of University data
- Acceptance/processing of credit or payment card transactions
- Design, creation, maintenance, support, and/or hosting of any website/webpage
- Transmission or storage of Personally Identifiable Information (PII) or Protected Health Information (PHI)
- Custom software development
- Software maintenance
- Hardware purchase with embedded software

UNC CHARLOTTE

Typical Technology Issues

What are we going to cover here?

- ✧ Privacy & statutory/regulatory compliance
  - FERPA/HIPAA/FACTA
  - PCI DSS
  - Section 504 & web accessibility
- ✧ Data & information security
- ✧ Ownership & use of data
- ✧ Electronic signatures
- ✧ Electronic documents
- ✧ Click-through agreements

UNC CHARLOTTE

Privacy & Compliance

How do I know what statutes, regulations, or industry standards are applicable?

- ? Will the vendor create, receive, maintain, or transmit Personally Identifiable Information (PII)? (FACTA)
- ? Will the vendor create, receive, maintain, or transmit Protected Health Information (PHI)? (HIPAA)
- ? Will the vendor receive, maintain, or transmit student education records? (FERPA)
- ? Will the vendor receive, maintain, or transmit credit card and/or debit card information? (PCI DSS)
- ? Will the vendor provide services that control or could impact the security of credit card and/or debit card information? (PCI DSS)
- ? Will the vendor supply electronic and information technology goods or services? (Section 504)

UNC CHARLOTTE

FACTA & PII

What the heck is FACTA?

- FACTA = Fair and Accurate Credit Transactions Act
- FTC issued regulations regarding identity theft prevention: "Red Flags Rule."
- Red Flags = suspicious patterns or practices or specific activities that indicate the possibility that identity theft may occur.
- University is required to implement a written Identity Theft Prevention Program (ITPP) designed to detect the warning signs ("red flags") of identity theft in its daily operations.
- All departments, colleges, and units who are involved with handling Personally Identifiable Information (PII) must comply with the University's ITPP and develop reasonable processes and procedures to verify the identity of persons for whom services are being provided and to detect, prevent, and mitigate any instances of identity theft.

What the heck is PII?

Any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including, but not limited to:

- name;
- address;
- telephone number;
- social security number;
- date of birth;
- government-issued driver's license or identification number;
- passport number;
- taxpayer identification number;
- credit, debit, or banking account numbers;
- unique electronic identification number, including IP or other computer identifying address; and
- unique biometric data such as fingerprint, voice print, retina or iris image or other unique physical representation.

UNC CHARLOTTE

PII

When would a vendor have access to PII?

- Vendor develops software to assist Advancement in fundraising activities: vendor may have access to PII of alumni/donors such as names, home mailing addresses, personal telephone numbers and financial account information.
- Vendor develops or upgrades physical access control systems (e.g., card swipe entry readers): vendor may have access to any PII collected via the card swipe such as names, social security numbers, and student ID numbers.

UNC CHARLOTTE

PII

So what does the contract need to say?

If you engage a vendor to perform an activity in connection with a University account that has PII, require in the contract that:

- the vendor has policies and procedures designed to detect, prevent and mitigate the risk of identity theft; and
- the vendor review the University's Identity Theft Protection Program and report any Red Flags to the Program Administrator.

UNC CHARLOTTE

FERPA

What the heck is FERPA?

Family Educational Rights and Privacy Act: Requires that "education records," including almost all University records related directly to a student, be held in confidence.

- Student access to own records
- Directory information exception
- Legitimate educational interest exception
- Consent exception
- University Policy 402, Education Records
- FERPA Resources

UNC CHARLOTTE

FERPA

What the heck is Directory Information?

- Information in a student's education record that would not generally be considered harmful or an invasion of privacy if disclosed. At UNC Charlotte, directory information consists of the student's name, major field of study, dates of attendance, enrollment status, and degrees and awards (including scholarships) received.
- Photographs, videos, or other media containing a student's image or likeness (collectively, "student images") and University-issued student electronic mail addresses ("email addresses") are designated by UNC Charlotte as "limited use directory information." Use and disclosure restricted to: (1) publication in official University publications or on University social media sites or websites; (2) University officials who have access to such information and only in conjunction with a legitimate educational interest; and (3) external parties **contractually affiliated** with the University, *provided such affiliation requires the sharing of limited use directory information.*

UNC CHARLOTTE

FERPA

When would a vendor have access to student education records?

- Vendor offers services such as an online performance, grading, testing, or discussion tools that require disclosure of education records to the vendor.
- Vendor offers a plagiarism detection tool for student work.

UNC CHARLOTTE

FERPA

So what does the contract need to say?

If you engage a vendor to provide a product or service that involves student education records:

- Explicitly provide that the vendor is an agent with a legitimate educational interest in the specific education records to which it may have access under the contract.
- Require in the contract that the vendor agrees to comply with the Family Educational Rights and Privacy Act (FERPA) and its regulations to the extent it has access to student education records.

UNC CHARLOTTE

HIPAA

What the heck is HIPAA?

Health Insurance Portability & Accountability Act

- Requires the University's health care components to protect against unauthorized use or disclosure of individually identifiable health information (specifically “Protected Health Information" or "PHI").
- PHI is health information, including demographic information, created or received by the University's health components which relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual **and that identifies or can be used to identify any individual**. (PHI does not include education records subject to FERPA or de-identified PHI.)
- University Policy 605.2, Privacy and Confidentiality of Individually Identifiable Health Care Information under HIPAA

When would a vendor have access to PHI?

- Vendor provides a product or service such as maintaining or transmitting Student Health Center records.
- Vendor provides product or service that requires use of PHI provided to the University by a third party health care provider.

UNC CHARLOTTE

HIPAA

So what does the contract need to say?

If you engage a vendor to provide a product or service that involves PHI:

- Require in the contract that the vendor agrees to comply with HIPAA; and
- If we are sharing PHI with the vendor, vendor must sign a Business Associate Agreement (BAA).

OLA can provide specific language and BAA.

UNC CHARLOTTE

PCI DSS

What the heck is PCI DSS?

Payment Card Industry Data Security Standard

- NC Office of State Controller and UNC Charlotte banking contracts state that the University is subject to PCI DSS and required to meet standards.
- ITS has numerous standards including:
  - Payment card processing standard
  - Payment processing procedures

UNC CHARLOTTE

PCI DSS

So what does the contract need to say?

If you engage a vendor to provide a product or service in connection with a University account that involves payment cards:

- Require in the contract that the vendor agrees to meet PCI DSS.

OLA or Purchasing can provide specific language.

UNC CHARLOTTE

Section 504

What the heck is Section 504?

- Section 504 of the Rehabilitation Act requires the University to make all programs and activities accessible to individuals with disabilities, including when our programs or activities are delivered via electronic means.
- Section 508 of the Rehabilitation Act provides standards for accessibility of technology, including computer hardware and software, websites, phone systems, and copiers.
- When websites follow Web Content Accessibility Guidelines (WCAG), they are accessible to all users and compatible with assistive technology, such as screen readers.
- UNC Charlotte Web Accessibility Standards & Guidelines

UNC CHARLOTTE

Section 504

When would a vendor need to comply with Section 504?

- Vendor provides software to the University for use by its students or employees.
- Vendor provides web-based services to the University for use by its students or employees.

UNC CHARLOTTE

Section 504

So what does the contract need to say?

Ensure that the following language is inserted into all contracts for the purchase of electronic and information technology goods or services:

> "Contractor warrants that its product or service complies with Section 508 of the Rehabilitation Act of 1973, as amended, and WCAG 2.0 AA with respect to accessibility for individuals with disabilities. In the event that the University receives any complaints or concerns regarding the accessibility of the product or service, Contractor agrees promptly to respond to and resolve those concerns. Further, Contractor agrees to indemnify and hold University harmless for any claims arising from the inaccessibility of its product or service."

UNC CHARLOTTE

Data & Info Security

What to look for in contracts related to:

- ✧ Public Records
- ✧ Security Practices
- ✧ Security Breach
- ✧ Data Protection

UNC CHARLOTTE

Data & Info Security

Public Records: What are they?

- "Public records" are all records created or received in the course of University business, in whatever format, including all documents, papers, letters, maps, books, photographs, films, sound recordings, magnetic or other tapes, electronic data-processing records, artifacts, or other documentary material, regardless of physical form or characteristics, made or received pursuant to law or ordinance in connection with the transaction of public business by the University. Note that the physical location of the records is inconsequential and that records on your personal devices (computers, smart phones, etc.) are still public records.
- *Exceptions:*
  - Personnel records (defined)
  - Student education records under FERPA
  - PHI under HIPAA
- University Policy 605.8, Public Records Requests

UNC CHARLOTTE

Data & Info Security

Public Records

If the contract includes the transfer/maintenance/storage of public records, does the vendor agree that the data will be…

- electronically and physically secure and backed up?
- accessible for public records requests (within 24-48 hours usually)?
- returned to us in a useable form at termination of contract?

We can't accept clauses that permit deletion of our records for non-payment or breach!

UNC CHARLOTTE

Data & Info Security

Security Practices

If contract includes transfer/maintenance/storage of University data, does the vendor agree to…

- adhere to security best practices for system development and maintenance?
- maintain current software versions and to patch regularly?
- fix/patch information security deficiencies or bugs in its or subcontractors' service/software in a timely fashion? (Contracts frequently use the term “commercially reasonable.”)
- notify University within 24 hours of major/significant issues? Does the contract define major/significant?

UNC CHARLOTTE

Data & Info Security

Security Breach

If contract includes transfer/maintenance/storage of University data, does the vendor agree to…

- notify University within 48 hours of an information security incident or breach that has likely compromised or involves inappropriate access to University data?
- assume liability for costs of investigating, responding/mitigating an information security breach due to failure to conform to the contract's terms? *(Note that NC AG controls any legal proceedings involving the University.)*
- indemnify University and faculty/staff against legal actions/third party claims, including costs and fees?
- add the University as an "additional insured" party to the vendor's insurance to cover potential breach costs?

UNC CHARLOTTE

Data & Info Security

Data Protection

If contract includes transfer/maintenance/storage of University data, does the vendor agree…

- to acknowledge responsibility to protect University data for itself and subcontractors, continuing after termination of the contract?
- that obligations survive the termination of the agreement?
- expedite return of all University data or destroy the data, including backup copies, within a specified time period after termination of agreement? (It is reasonable to allow an extended period for destruction of backup data.)
- to return the data at the University's request?
- to return data in a commonly readable format?

UNC CHARLOTTE

Ownership & Use of Data

Data Rights

- If vendor will produce, furnish, acquire, or use University data, make sure contract contains terms that delineate the respective rights and obligations of the University and the vendor/contractor regarding the use, reproduction, and disclosure of that data.
- University Policy 315, Copyright Policy
- University Policy 308, Research Relations with Private Enterprise and Publication of Research Findings

UNC CHARLOTTE

Ownership & Use of Data

Protected Data

When the vendor technology or service involves protected data (under NC or US law), the vendor must agree to…

- acknowledge that access to protected data exists,
- agree to use protected data only for purposes of their service,
- agree to return or destroy the data upon termination of the contract,
- agree to take responsibility for the protected data and its obligations to protect the data, and
- agree to report unauthorized disclosure or misuse of protected data.

- *Use one-page Data Protection Agreement (available from OLA)*

UNC CHARLOTTE

Electronic Signatures

Guidelines for accepting digital or electronic signatures

https://legal.uncc.edu/legal-topics/contracts/guidelines-accepting-digital-or-electronic-signatures

NC law recognizes validity of electronic or digital signatures for contracts, but several criteria must be met:

- Both parties must agree that utilizing digital or electronic signatures is acceptable.
- If any unit head or supervisor does not want to accept a digital or electronic signature from the other party, he/she may make that decision for the unit and require hard copy documents with original handwritten ink signatures.

UNC CHARLOTTE

Electronic Signatures

Acceptable digital/electronic signatures

- A handwritten signature on a document is valid, including when the entire document is scanned or faxed to the University.
- A graphic image of a signature placed on a document using secure software that verifies the identity of the user on the other end (*e.g.* DocuSign) is valid.
- For student or employee signatures, marks, initials, or checkboxes are valid ONLY if:
  - The student or employee is required to log in to the signature form utilizing their NinerNet credentials; AND
  - The electronic signature is captured in a secure audit trail that provides clear, easily producible evidence that the student or employee logged in with their NinerNet credentials and indicated their assent.

UNC CHARLOTTE

Electronic Signatures

Unacceptable “signatures”

- A graphic image of a signature placed on a document and not verified by secure software. (See next slide.)
- A typewritten name, regardless of font, that has not been verified by secure software or through NinerNet.

UNC CHARLOTTE

Electronic Signatures

DATA PROTECTION AGREEMENT

This Data Protection Agreement ("Agreement") is entered into as of the date last signed ("Effective Date") between _____, a _____ ("Contractor"), and The University of North Carolina at Charlotte, an institution of higher education ("University"). University and Contractor are referred to jointly as the "Parties" or singularly as a "Party." Contractor and University agree as follows:

1. **Purpose.** The purpose of this Agreement is to establish the content, use, and protection of Protected Data needed by Contractor to support certain services provided to University by Contractor.

2. **Protected Data.** For the purposes of this Agreement, "Protected Data" is defined as information that is provided by University to Contractor or collected by Contractor on behalf of University and that is protected by Federal or North Carolina law.

3. **Term.** This term of this Agreement shall begin as of the Effective Date and shall end upon the termination of all outstanding service agreements between the Parties.

4. **Constraints on Use of Protected Data.** Protected Data supplied by University to Contractor or collected by Contractor on behalf of University is the property of University and shall not be sold or used by Contractor, internally or externally, for any purpose not directly related to the scope of work outlined in a written agreement between the Parties without the written permission of University.

5. **Protected Data Security.** Contractor shall employ industry best practices, both technically and procedurally, to protect Protected Data from unauthorized physical and electronic access. Methods employed are subject to review and approval by University.

6. **Compliance with Law.** Contractor shall comply with, and shall not cause University to violate, applicable Federal and North Carolina laws and regulations protecting the privacy of citizens including, but not limited to, the Family Educational Rights and Privacy Act ("FERPA"), the Health Insurance Portability and Accountability Act ("HIPAA") and the Financial Services Modernization Act (the "Gramm-Leach-Bliley Act").

7. **Notification of Security Breaches.** The North Carolina Identity Theft Protection Act of 2005 (N.C. Gen. Stat. § 75-60 et seq., as applied by N.C. Gen. Stat. § 132-1.10(c1)) delineates notification requirements in the event of a breach in the security of personal information. Contractor agrees that in the event of any breach or compromise of the security, confidentiality or integrity of any data where personal information of a University student, prospective student, employee, alumnus or other University-affiliated person or entity was, or is reasonably believed to have been, acquired and/or accessed by an unauthorized person and where such breach is known to Contractor or upon notification of such breach to Contractor, Contractor shall notify University of such breach or compromise within 24 hours, comply with all notification actions and assist University with all notification actions required by University policy and applicable law.

8. **Destruction of Protected Data.** Upon termination of all outstanding service agreements between the Parties, Contractor shall return to University all Protected Data. Contractor shall certify in writing within five business days that all copies of Protected Data stored on Contractor servers, backup servers, backup media, or other media including paper copies have been permanently erased. For the purposes of this provision, "permanently erased" means the Protected Data have been completely overwritten and are unrecoverable.

IN WITNESS WHEREOF, the Parties have executed this Agreement as of the Effective Date.

Contractor:

By: _____
(Signature of Authorized Representative)

University:

The University of North Carolina at Charlotte

By: _____

Not valid!

UNC CHARLOTTE

Electronic Documents

What format is an “original” electronic contract?

When a contract will be transmitted in electronic form (PDF or fax):

- Add this clause: "This Agreement may be executed in counterparts, each of which shall be deemed an original. Facsimile copies or Adobe Portable Document Format (PDF) copies sent by email shall be considered for all purposes as originals.”
- Require that the entire document be part of a single .pdf rather than piecemeal, so it is clear what the other party agreed to and signed.

UNC CHARLOTTE

Click-Through Agreements

"A contract is no less a contract simply because it is entered into via a computer."

Forrest vs. Verizon Communications Inc., 805 A.2d 1007 (D.C. 2002)
(addressing the validity of a forum selection clause)

- Adhesion contract = Need the service; no choice but to agree to terms
- Unilateral contract = Express assent is obtained by one side clicking "Agree"
  - generally considered binding, provided not unconscionable or otherwise unenforceable

UNC CHARLOTTE

Click-Through Agreements

BEWARE!

While you may think click-through agreements are harmless and common, terms will usually be enforceable, and person who clicks may be personally liable (if not authorized by the University to sign).

- Best to read through before you click, and consult with Purchasing.
- Common terms you don't want to agree to:
  - Mandatory arbitration
  - Indemnity/hold harmless
  - Governing law/jurisdiction/forum other than NC
  - Limitation of liability

UNC CHARLOTTE

Questions?

UNC CHARLOTTE

Resources

UNC Charlotte Resources

- **Contract Checklist** https://legal.uncc.edu/legal-topics/contracts/contract-checklist
- **General Contract Information & Resources** https://legal.uncc.edu/legal-topics/contracts
- **IT Standards & Guidelines** http://itservices.uncc.edu/home/it-policies-standards/standards-and-guidelines
- **Purchasing** http://finance.uncc.edu/about-us/materials-management/purchasing
- **Red Flags Rule Information (Financial Services)** http://finance.uncc.edu/resources/manuals-guides-procedures/red-flags-rule

UNC CHARLOTTE

Resources

University Policies & Regulations on Data & Information Security

- UP 311, Information Security
- UP 311.2, GLBA Information Security Program Regulation
- UP 311.4, Peer-to-Peer File Sharing Regulation
- UP 311.5, Personal Information Security Breach Notification Procedures
- UP 311.6, Regulation on Security of Electronic Individually Identifiable Health Care Information under HIPAA
- UP 311.7, Regulations on Information Systems Security
- UP 311.8, Regulations on the Use of Social Security Numbers
- UP 311.9, Regulation Regarding Third Party Data Subject to Contractual Access Restrictions

UNC CHARLOTTE

Resources

Electronic Signatures

- NC Electronic Commerce in Government Act NCGS § 66-58.1, *et seq*.
- NC Sec'y of State administers Electronic Commerce Act https://www.sosnc.gov/ecomm/
- DocuSign is NC govt's exclusive e-signature provider (UNC Charlotte did not purchase and does not use for its own contracts)
- NC Uniform Electronic Transactions Act, NCGS § 66-311
- NC e-procurement: http://eprocurement.nc.gov/

UNC CHARLOTTE

Credits

(Why reinvent the wheel?)

- **Information Security Questions for Contract Review, University of Minnesota, Information Technology** https://it.umn.edu/information-security-questions-contract
- **University of Nebraska – Kearney, Technology Contract Guidelines** https://www.unk.edu/offices/its/its_main_page_tabs-files/guidelines/2016-technology-contract-guidelines.pdf
- **UAB IT Related Contracts and Agreements** https://www.uab.edu/it/home/it-reports-and-publications/item/321-it-related-contracts-agreements
- **University of Pittsburgh, Guide to Identifying PII** http://technology.pitt.edu/security/guide-to-identifying-personally-identifiable-information-pii