Protecting Research Data

Micki Jernigan, Chief Privacy Officer, ITS

Larry Fritsche, Senior Security Operations Manager, ITS

Brian Penders, Chief Information Security Officer, School of Medicine

October 17, 2019

Agenda

- Introduction
- Defining Sensitive Information (SI)
- IRB data security requirements
- Best practices for storing and sharing SI
- HIPAA and NC ID Theft Protection Act
- Purchasing process

Introduction

Defining Sensitive Information

- Tier 0: Public Information
- Tier 1: Business Information
- **Tier 2: Confidential Information**
- **Tier 3: Restricted Information**

https://its.unc.edu/files/2016/01/STANDARD-Information-Classification.pdf

Defining Sensitive Information

- **Tier 2:** Confidential Information is the default classification of University information until determined otherwise. Confidential Information includes information which the University is required by law, regulation, contract, policy, or other governing requirement to keep confidential.
- **Tier 3:** Restricted Information: includes any information that the University has a contractual, legal or regulatory obligation to safeguard in the most stringent manner. Unauthorized disclosure or loss of this information may require notification.

https://its.unc.edu/files/2016/01/STANDARD-Information-Classification.pdf

IRB Data Security Requirements

Level 1 (***should be***) and Level 2 (***must be***) protected by:

1. Password complexity
2. Secure network
3. Endpoint protection
4. Patch management
5. Lowest level of privilege

https://research.unc.edu/files/2017/02/DataSecurityLevels_I_through_III_20170222.pdf

IRB Data Security Requirements

Level 3 (**must also**) be protected by:

6. Encryption
7. Vulnerability Scanning
8. Information Security Control Standard

https://research.unc.edu/files/2017/02/DataSecurityLevels_I_through_III_20170222.pdf

Best practices for storing and sharing SI

- OneDrive is the best option (rated for SI, all activity is logged, allows external sharing, etc.)
- Email ('secure' in subject) option ensures encryption in transit but no persistent protection for attachments
- Native encryption available in OWA and Outlook clients

Best practices for storing and sharing SI

- https://safecomputing.unc.edu/
- Safe travel recommendations included as well

Secure Texting

- SMS texting is not a secured form of communication per HIPAA security requirements. Unfortunately, there is no approved texting vendor for HIPAA (PHI) at UNC-CH.
- Texting is a transmission service and therefore requires a security risk assessment of any product or vendor (and approval) prior to use and possibly a Business Associate Agreement (BAA) with that vendor if PHI is involved.

Secure Texting

- The School of Medicine Information Security Office is currently working with the Institutional Privacy Office on reviewing a secure text messaging solution, but that effort is in the early phases.

HIPAA

Why does HIPAA apply to the University?

The University is a hybrid **"Covered Entity"** because certain units furnish, bill, receive payment for health care services, or may have access to PHI in the normal course of business.

Covered University Units ("CUUs"), and their faculty, staff, students, volunteers and others working in these units (employees), that use or disclose PHI must comply with HIPAA.

Protected Health Information (PHI)

PHI is any information that can be used to identify an individual – whether living or deceased*– that relates to the individual's past, present, or future physical or mental health condition, including health care services provided, and payment for those services.

*HIPAA protects the PHI of a **deceased individual for 50 years following death**.

What does PHI look like?

Written.

Spoken

Electronic

It is the responsibility of ALL University staff, faculty, student, volunteer or other individual granted access to PHI including YOU, to protect the privacy and security of PHI in ALL forms.

PHI Identifiers

If any **1** of these **18** identifiers exists in connection with a person's health information, it is PHI and must be protected.

Note: **If ALL 18 identifiers are removed** for the person **AND the person's** relatives, household members, & employers, then the information does not have to be protected.

1. **Names (including initials)**
2. **Geographic subdivisions (smaller than a state)**
3. **Dates (except year)**
4. **Telephone numbers**
5. **Fax numbers**
6. **E-mail addresses**
7. **Social Security numbers (full or partial)**
8. **Medical record numbers**
9. **Health plan beneficiary numbers**
10. **Account numbers**
11. **Certificate/license numbers**
12. **Vehicle identifiers/ serial numbers**
13. **Device identifiers/ serial numbers**
14. **Web URLs**
15. **IP address numbers**
16. **Biometric identifiers (fingerprints or voiceprints)**
17. **Full face photographs or images**
18. **Any other unique number, code, or characteristic that can be linked to an individual**

Research

HIPAA regulates how PHI may be obtained from a covered entity and used for research.

This is true whether the PHI is completely identifiable or partially de-identified in a limited data set (LDS). A HIPAA compliant DUA is required for a LDS. De-identified requirements under HIPAA may not be the same as under the Common Rule. ALL 18 identifiers and derivatives must be removed to be de-identified per HIPAA.

A researcher or healthcare provider is not entitled to use PHI in research without the appropriate documentation, including an individual patient authorization or an institutionally approved waiver of authorization.

A valid HIPAA Authorization form is required even if a potential research subject has signed an Informed Consent Form.

Report Potential Compromises Immediately

If PHI is suspected of being mishandled, lost, stolen, improperly accessed, or disclosed it is potentially compromised and potentially at risk and must be reported immediately, **even if by mistake**.

Your responsibility is to report a **potential compromise to your supervisor AND one of the following**:

- your HIPAA Privacy Liaison
- your Information Security Liaison
- the Chief Privacy Officer
- the Chief Information Security Officer
- the Office of University Counsel

Faculty, staff, volunteers, students, or contractors of the University may not threaten or take any retaliatory action against an individual for exercising his or her rights under HIPAA or for filing a HIPAA report or complaint.

Disciplinary Action

If you **violate HIPAA or University policy**, you will be subject to **appropriate disciplinary action** as outlined in the University's policies, standards, and guidelines, including the HIPAA Sanctions Standard.

You may also be subject to **criminal or civil penalties**.

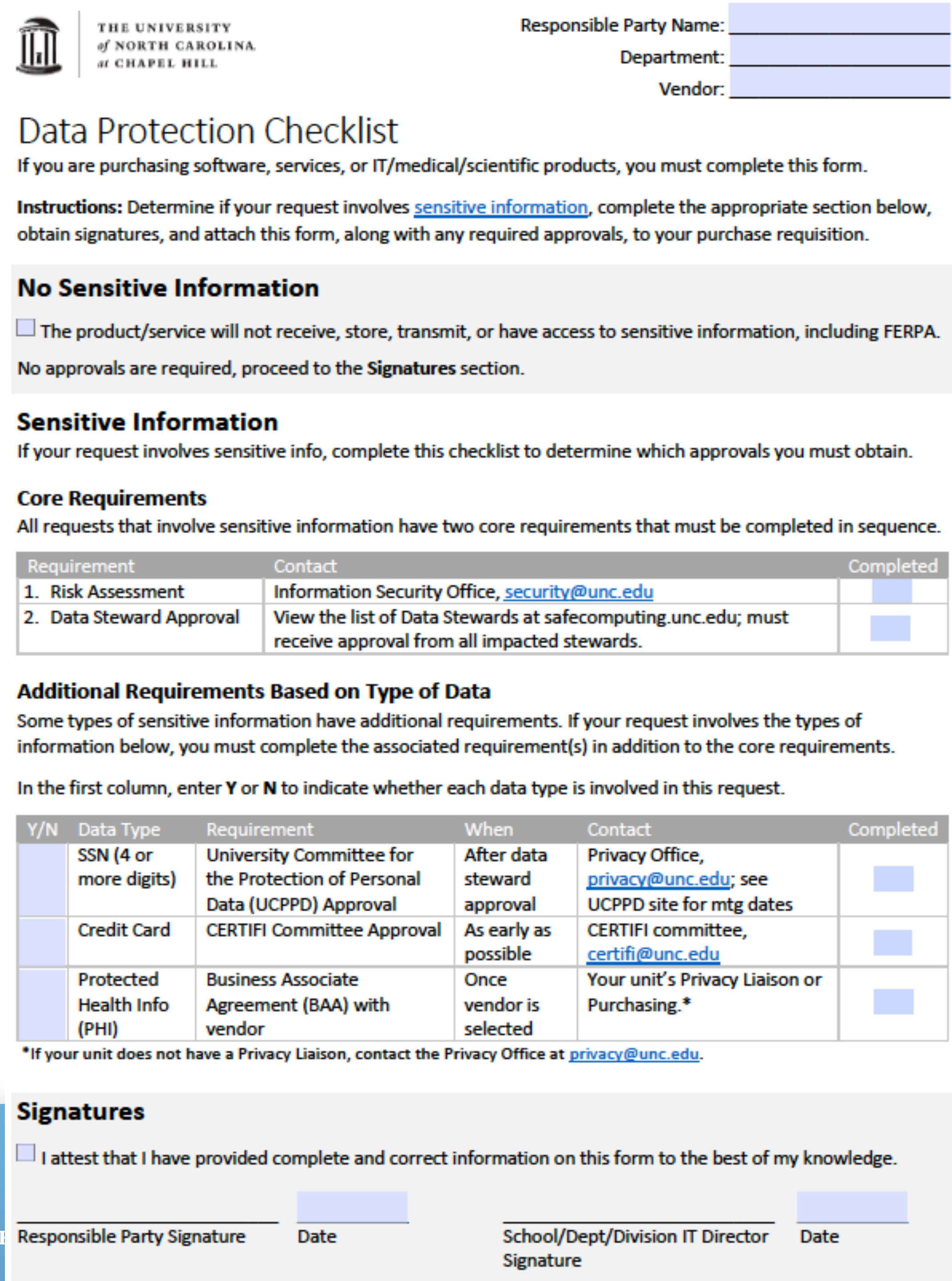
NC Identity Theft Protection Act

First Name or Initial and Last Name with one or more of:

- SSN or employer tax id number
- Drivers license, State identification card, or passport numbers
- Checking account numbers
- Savings account numbers
- Credit card numbers
- Debit card numbers
- Personal Identification (PIN) Code as defined in G.S. 14-113.8(6)
- Electronic identification numbers, electronic mail names or addresses, Internet account numbers, or Internet identification names
- Digital signatures
- Any other numbers or information that can be used to access a person's financial resources
- Biometric data
- Fingerprints
- Passwords
- Parent's legal surname prior to marriage

Purchasing Process

- Data Protection Checklist
- Risk Assessment
- Business Associate Agreement
- UCPPD review



THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL

Responsible Party Name: ____________

Department: ____________

Vendor: ____________

Data Protection Checklist

If you are purchasing software, services, or IT/medical/scientific products, you must complete this form.

Instructions: Determine if your request involves sensitive information, complete the appropriate section below, obtain signatures, and attach this form, along with any required approvals, to your purchase requisition.

No Sensitive Information

□ The product/service will not receive, store, transmit, or have access to sensitive information, including FERPA.

No approvals are required, proceed to the **Signatures** section.

Sensitive Information

If your request involves sensitive info, complete this checklist to determine which approvals you must obtain.

Core Requirements

All requests that involve sensitive information have two core requirements that must be completed in sequence.

Requirement	Contact	Completed
1. Risk Assessment	Information Security Office, security@unc.edu	
2. Data Steward Approval	View the list of Data Stewards at safecomputing.unc.edu; must receive approval from all impacted stewards.	

Additional Requirements Based on Type of Data

Some types of sensitive information have additional requirements. If your request involves the types of information below, you must complete the associated requirement(s) in addition to the core requirements.

In the first column, enter **Y** or **N** to indicate whether each data type is involved in this request.

Y/N	Data Type	Requirement	When	Contact	Completed
	SSN (4 or more digits)	University Committee for the Protection of Personal Data (UCPPD) Approval	After data steward approval	Privacy Office, privacy@unc.edu; see UCPPD site for mtg dates	
	Credit Card	CERTIFI Committee Approval	As early as possible	CERTIFI committee, certifi@unc.edu	
	Protected Health Info (PHI)	Business Associate Agreement (BAA) with vendor	Once vendor is selected	Your unit's Privacy Liaison or Purchasing.*	

*If your unit does not have a Privacy Liaison, contact the Privacy Office at privacy@unc.edu.

Signatures

□ I attest that I have provided complete and correct information on this form to the best of my knowledge.

____________________ Responsible Party Signature

________ Date

____________________ School/Dept/Division IT Director Signature

________ Date

Risk Assessment

- A risk assessment reviews software, products, and/or services to evaluate the potential for loss or harm as it relates to information security. Any system that creates, receives, maintains, or transmits University-owned sensitive information OR that is considered mission-critical must have a risk assessment.

Business Associate (BA)

A BA is generally a company or individual outside of the University that creates, receives, maintains, or transmits PHI on behalf of the University.

- Example: a cloud service provider storing electronic PHI
- Equipment for clinical use that stores, transmits, etc. PHI

A BA must sign a **Business Associate Agreement ("BAA")** with the University and adhere to the HIPAA Privacy, Security and Breach Notification Rules

Units within the University may be BA's of external entities. When a BAA is necessary for this purpose, the same process for obtaining the agreement is required.

Business Associate Agreement (BAA)

- The University has template BAAs that it uses.

- Once you obtain the signed BAA, you must **submit the signed BAA**, any supporting documents, and the underlying agreement to the **BAA repository**, available on the Institutional Privacy Office's website, privacy.unc.edu (Onyen-protected).

- Your unit should also retain a copy of these documents.

- If you are unsure if you need a BAA or have other questions regarding BAAs, please contact your unit's Privacy Liaison. If your unit does not have a Privacy Liaison, please contact the Institutional Privacy Office.

University Committee for the Protection of Personal Data (UCPPD)

UCPPD reviews and approves:

- all access, use, and disclosure of Social Security numbers (full or partial) at the University
- Red Flags Rules requirements
- Identity Theft program requirements

Questions?

privacy@unc.edu

security@unc.edu

help@med.unc.edu