Appendix DS

Why Appendix DS?

- To help ensure that UC Institutional Information (the data) and IT Resources (the systems) are kept secure when shared with or access is provided to third-parties.
  - Cloud services
  - Consultants
  - Service/Maintenance Contracts
- Appendix DS applies to:
  - All UC Data (P1 through P4)
  - All purchase amounts from “free” services to multi-million dollar purchases
  - All payment methods including PALCards and purchase orders
- **Does not apply to software only installed and used locally**
  - **This line can be a bit blurry…**

Components of Appendix DS

- Appendix DS Contract Terms
  - Purpose and Introduction
  - Defined Terms
  - Requirements
- Exhibit 1 - Institutional Information
  - Filled out by the requesting Unit in consultation with Security, Privacy, and other SME's as needed
  - Used to inform the Supplier of the types of data involved in the contract and any legal, regulatory, or contract security requirements
- Exhibit 2 – Supplier's Initial Information Security Plan
  - More on this later…

Appendix DS Requirements in a Nutshell

Suppliers must:

3) Agree to protect our data and not sell it or use it for other purposes without our permission
4) Have a documented security plan that we can evaluate
5) Have some evidence that they are following their own security plan
6) Tell us if they make major changes to their security plan, security posture, or have any significant security vulnerabilities in their environment
7) Agree to return and/or delete our data when the contract ends
8) Tell us (if they are legally allowed to do so) if there are any legal requests for our data
9) Tell us if our data is breached, work with us to investigate, and bear notification and other costs as appropriate. A breach can also be grounds for termination.
10) Agree not to install backdoors or other illicit code in software or systems
11) Agree to perform appropriate background checks on employees that have access to our systems or data

Exhibit 1 in a Nutshell

Three Sections

1. Protection Level
   - Determines the applicable cyber security insurance requirements in the Terms and Conditions
2. Institutional Information data element descriptors
   - What kind of data is this anyway?
3. Institutional Information Regulation or Contract Requirements
   - What are the big legal requirements, regulations, or contract requirements that may/will:
     - Inform the Supplier on how they need to protect the data
     - Determine how UCI negotiates the contracts including Appendix DS and evaluates the Supplier Security Plan
   - Document other requirements as appropriate

Exhibit 1, Protection Levels

1. Protection Level Classification[4]:

- ☐ Protection Level 1
- ☐ Protection Level 2
- ☐ Protection Level 3
- ☐ Protection Level 4

- Refer to Protection Level guidance below. More than one may apply.
- Use the **Classification Decision Tree** to help guide classification decisions
- Provide a short description on what the data is and how it's used

https://security.uci.edu/security-plan/plan-classification.html

https://security.ucop.edu/policies/institutional-information-and-it-resource-classification.html

Exhibit 1, Data Element Descriptors

2. Institutional Information data element descriptors:

Select all data types that apply:

A. ☐ Animal Research Data.
B. ☐ Controlled Technical Information (CTI).
C. ☐ Controlled Unclassified Information (CUI) – 800-171/NARA.
D. ☐ Defense Department: Covered Defense Information (CDI).
E. ☐ Federal Acquisition Regulations (FARS/DFAR) other than CUI.
F. ☐ GDPR personal data.
G. ☐ GDPR special data.
H. ☐ Health data – other identifiable medical data not covered by HIPAA. (Including but not limited to: occupational health, special accommodation, or services qualification, etc.)
I. ☐ Health Records subject to HIPAA Privacy or Security Rule (PHI).
J. ☐ Human Subject Research Data.
    1. ☐ Identified.
    2. ☐ Anonymized.
K. ☐ Intellectual property (IP), such as patents, copyright, or trade secrets.
L. ☐ ITAR/EAR-controlled data.
M. ☐ Payment card data (PCI, PCI DSS).
N. ☐ Personally identifiable information – PII.
O. ☐ Student data, whether or not subject to FERPA.

Common Data Elements

- Personally Identifiable Information (PII)
  - Can be P1 though P4
  - Very broad legal definition but can include any detail collected about an individual including names, physical addresses, phone numbers, e-mail address, birthday, physical descriptions, etc.
  - Also includes P4 elements such as SSN, driver's license numbers, credit card numbers, medical information, account names and passwords, etc.
- Health Records subject to HIPAA Privacy or Security Rule (PHI).
  - Protected Health Information (PHI) linked to an individual that is created, collected, transmitted, or maintained by a HIPAA Covered Entity or Business Associate in relation to health care, payments, or healthcare operations
  - **BAA will be required in addition to Appendix DS**
- Health Data – other identifiable medical data not covered by HIPAA
  - Most other medical info including disability services, occupational health, special accommodations, workplace medical documentation, etc.
  - Most medical data used for research falls into this category

Common Data Elements

- Student data, whether or not subject to FERPA
  - More on FERPA later…
- Payment card data (PCI, PCI DSS)
  - All credit card processing activities
    - Especially in cases where UCI is considered the Merchant of Record
  - Additional PCI requirements for all Suppliers involved with card processing
- GDPR Personal Data
  - Very broad category of PII associated with EU residents
- GDPR Special Data
  - Sensitive data on EU residents including racial or ethnic origins, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, or data concerning a natural person's sex life or sexual orientation

Research Data Elements

- Lots of different types of research data with **additional contract requirements**. Work with your **faculty member** to see if any of these data types are appropriate:
  - Animal Research Data
  - Controlled Unclassified Information (CUI), Defense Department: Covered Defense Information (CDI), and Controlled Technical Information (CTI)
    - Data from the federal government subject to NIST 800-171 requirements
  - Federal Acquisition Regulations (FARS/DFAR) other than CUI
    - Specific federal or DoD regulations
  - Human Subject Research Data
    - Federal protocols usually part of campus IRB review
    - Can be identified or anonymized
  - ITAR/EAR controlled data
    - Export controls relating to sensitive technology and national security
  - Intellectual property (IP), such as patents, copyright, or trade secrets

Exhibit 1, Regulations and Contracts

3. Institutional Information Regulation or Contract Requirements:

Select all regulations or external obligations that apply to inform UC and the Supplier of obligations related to this Appendix:

Privacy (* indicates data security requirements are also present)

A. ☐ California Confidentiality of Medical Information Act (CMIA) *.
B. ☐ California Consumer Privacy Act (CCPA).
C. ☐ California Information Practices Act (IPA).
D. ☐ European Union General Data Protection Regulation (GDPR)*.
E. ☐ Family Educational Rights and Privacy Act (FERPA) *.
F. ☐ Federal Policy for the Protection of Human Subjects ("Common Rule").
G. ☐ Genetic Information Nondiscrimination Act (GINA).
H. ☐ Gramm-Leach-Bliley Act (GLBA) (Student Financial Aid) *.
I. ☐ Health Insurance Portability and Accountability Act/Health Information Technology for Economic and Clinical Health Act (HIPAA/HITECH) *.
J. ☐ Substance Abuse and Mental Health Services Administration SAMHSA (CFR 42 Part 2).
K. ☐ The Fair and Accurate Credit Transaction Act (FACTA).
L. ☐ The Fair Credit Reporting Act (FCRA).

Exhibit 1, Regulations and Contracts

Data Security

M. ☐ Chemical Facility Anti-Terrorism Standards (CFATS).

N. ☐ Defense Federal Acquisition Regulations (DFARS).

O. ☐ Export Administration Regulations (EAR).

P. ☐ Federal Acquisition Regulations (FARS).

Q. ☐ Federal Information Security Modernization Act (FISMA).

R. ☐ International Traffic in Arms Regulations (ITAR).

S. ☐ Payment card data (PCI, PCI DSS).

T. ☐ Toxic Substances Control Act (TSCA).

U. ☐ Other: _____

V. ☐ Other: _____

W. ☐ Other: _____

X. ☐ Other: _____

Common Laws and Regulations

- California Information Practices Act (IPA)
  - The primary data privacy law for California state government, including UC
  - Protections on how personal information is collected and managed
  - Notification requirements for breach of certain PII
- California Consumer Privacy Act (CCPA)
  - Enhanced privacy protections for California residents
  - Doesn't apply to UC directly but may apply to Suppliers we do business with
- Family Educational Rights and Privacy Act (FERPA)
  - Only applies to data considered part of the official student record
  - Student medical information is covered under FERPA
- European Union General Data Protection Regulation (GDPR)
  - Protects the personal information of EU residents
  - **GDPR Appendix is required in addition to Appendix DS**

Common Laws and Regulations

- HIPAA/HITECH
  - All PHI subject to the HIPAA Privacy and HIPAA Security Rules
  - Generally, does not include data used for research purposes
  - **Requires review by UC Health**
- California Confidentiality of Medical Information Act (CMIA)
  - Basically the California version of HIPAA
- Substance Abuse and Mental Health Services Administration SAMHSA (CFR 42 Part 2)
- Payment Card Data (PCI, PCI DSS)
  - All credit card processing activities
  - **Must be approved by the UCI PCI Committee**
  - **Appropriate Attestation of Compliance (AOC) required**
- Gramm-Leach-Bliley Act (GLBA)
  - Privacy of Student Financial Aid Information
  - May also be subject to NIST 800-171 requirements

Research/Other Regulations

- Federal Policy for the Protection of Human Subjects (“Common Rule”)
- Federal Acquisition Regulations (FARS)
- Defense Federal Acquisition Regulations (DFARS)
- International Traffic in Arms Regulations (ITAR)
- Export Administration Regulations (EAR)
- Federal Information Security Modernization Act (FISMA)
- Chemical Facility Anti-Terrorism Standards (CFATS)
- Toxic Substances Control Act (TSCA)
- Genetic Information Nondiscrimination Act (GINA)
- The Fair and Accurate Credit Transaction Act (FACTA)
- The Fair Credit Reporting Act (FCRA)

Challenges with Appendix DS

- Negotiating Appendix DS terms can be lengthy
  - Large companies often won't negotiate
  - Suppliers with smaller value contracts often don't want to negotiate either
  - Also be wary of Suppliers who accept terms too quickly
- Wide levels of security maturity among Suppliers
  - Many smaller to mid-size companies don't have formal security plans or third-party audits
  - The Higher Education Community Vendor Assessment Tool (HECVAT) can sometimes help bridge the gap
- Security risk assessment depth and final recommendation will depend on:
  - Completeness of the security plan and third-party audits
  - The Protection Level Requirements
  - The specific regulations and contract requirements needed for compliance
  - Security exception process and approvals may be needed for significant gaps

Improving Appendix DS

- One size does ***not*** fit all
- Small Suppliers have difficulty with formal security plans, background checks, and cyber security insurance
- Low-risk use cases may not need a full security risk assessment

- Future Plans:
  - Develop an Appendix DS Lite for low-risk use cases
  - Develop specific Risk Treatment Plans as a substitute for a formal Supplier security plan in low-risk use cases
  - Provide training and encourage UISL's to do risk assessments for P1-P2 use cases
  - Security Risk and Compliance is exploring the use of a GRC tool to streamline and document Supplier risk assessments
    - Better inventory of pre-approved Suppliers for specific use cases

Risk Driven Security Reviews

Security. Review Prior to Purchase	**EXEMPT** ➢ *No security review required prior to purchase.* ➢ *No Appendix DS required*	**LIGHT** Review ➢ ***Unit**-level review and discretion.** ➢ *Appendix DS required or comparable Supplier terms**	**FULL** Review ➢ *Detailed review by **OIT Security Risk & Compliance**.* ➢ *Appendix DS required or comparable Supplier terms*	**FULL** Review – HIPAA Scope ➢ *Detailed review by **UCI Health Security*** ➢ *Appendix DS required or comparable Supplier terms* ➢ *Business Associate Agreement (BAA) required*
Location + Prot. Level	• On premise (i.e., not Cloud) • P1, P2, P3, P4	• Cloud with P1/P2 data	• Cloud with P3/P4 data • Processes payments of any kind	• Cloud with HIPAA Data
Characteristics and Examples	Previously approved for similar use case.	UC directory level information (faculty, staff and students who have not requested a FERPA block)	Supplier will have access to UC P3/P4 resources (network, systems) or institutional information.	Information about health status, provision of health care, payment for health care created or collected by a Covered Entity (or a Business Associate of a Covered Entity), and can be linked to an individual.
	Supplier will not have access to UC resources (data, network, systems)	De-identified research data (in most cases)	Misuse of software could cause harm to life or property	Includes any part of a patient's medical record or payment history.
		Routine business records with P1/P2 data.	Software processes payments of any kind	UCI Health is a covered entity.
		Unpublished research work and intellectual property not classified as P3 or P4.	Financial information	Note: Information related to Student health falls under FERPA, not HIPAA.
		Does not integrate with Canvas	Human resource information	
		Supplier will have access to UC P1/P2 resources (network, systems) or institutional information.	Other sensitive medical information (not HIPAA)	
			Personally identifiable information	
			Canvas integrations	
			Student education records covered by FERPA.	
			Sensitive research	
			Routine business records with P3/P4 data.	