Data Classification Policy

Summary

All SUNY Cortland's data must be classified into one of the three categories described in this standard and protected using appropriate security measures consistent with the minimum standards for the classification level as described in related information security standards, procedures, and guidelines.

Applicability and Scope

This policy applies to all members of the SUNY Cortland community, as well as to external vendors and contractors who receive and maintain collections of College data.

Data Classification and Security Controls Requirements

All College data stored on College systems, or non-College owned resources where College business is transacted, must be classified into one of the three categories defined in the standard section of this document. Based on the data classification, Data Stewards, Data Custodians, and users are required to implement appropriate administrative, technical, and physical controls to protect the data utilizing the Data Classification Matrix Appendix D and Appendix E. Category-I data has more stringent requirements than Categories II and III. All systems require some protective measures.

When information from multiple classifications is co-located on the same system without effective means of isolation, or within the same repository, database, archive, or record, the minimum security controls of the category representing the highest institutional risk must be applied. As an example, if names and social security numbers were included in meeting minutes, then Category I protections would be required for that document.

These requirements exist in addition to all other College policies and federal and state regulations governing the protection of College data. Compliance with this requirement alone will not ensure that data will be properly secured. Rather, data classification should be considered an integral part of a comprehensive information security plan.

Note: Consistent with the notion of Incidental Use, personal data belonging to employees stored on a College resource is not considered College data.

Definitions

Category I: Protected Data -
Regulated private data includes: information defined as *private information* (i.e., personally identifiable information) in the New York State Information Security Breach and Notification Act of 2005: i.e., bank account/credit card/debit card numbers, Social Security Numbers, state-issued drivers' license numbers, and state-issued non-drivers' identification numbers. Additionally, SUNY Cortland declares protected health information (PHI), administrative authentication credentials, and passport numbers as Category 1 data.

The Breach Notification Act requires that the College must disclose any breach of the data to NY residents. (State entities must also notify non-residents. See New York's Information Security Policies at https://www.its.ny.gov/eiso/policies/security .

Regulated protected data includes data protected by state and federal regulations. This includes FERPA-protected educational records, protected health information (HIPAA), and other records governed by state and federal laws and regulations

Note that Category I data is exempt from disclosure/release under the NY State Freedom of Information Law (FOIL) (https://www.dos.ny.gov/coog/foil2.html). Such data must be appropriately protected to ensure that they are not disclosed in a FOIL request. FOIL excludes data that if disclosed would constitute an unwarranted invasion of personal privacy. Specific details on FOIL-excluded data are provided in the Appendix.

Category II: Internal Use Data - Includes College non-public data not included in Category I (Personally Identifiable or Regulated). Internal Use data includes Cortland ID, licensed software, as well as College business records, intellectual property, certain types of information that would constitute an unwarranted invasion of personal privacy, and any non-public data that would generally require a FOIL request prior to release.

Category III: Public Data - General access data, such as that available on unauthenticated portions of www.cortland.edu Category III data has no special requirements for confidentiality.

The Standard

The objective of this standard is to assist Data Stewards, their designees, and Data Custodians in determining the level of security required to protect data for which they are responsible. The standard divides data into three categories:

Data Classification	Risk from Disclosure	Description	Examples
Category I: Protected Data	High-Medium	Personally Identifiable data includes information whose unauthorized access or loss could seriously or adversely affect SUNY Cortland; an authorized, contracted partner; specific individuals, or the public. Security breaches of this information are subject to the NY State Information Security and Breach Notification Act and other federal, state, and industry rules and regulations. Regulated data includes information subject to FERPA or other federal, state, or business regulations (e.g., HIPAA, Red Flag Rules) that require specific levels of protection to prevent its unauthorized modification or use.	**Statutory Data** • Social Security Number • Driver's License Number • DMV State-issued Non-drivers ID Number • Bank/Financial Account Number • Credit/Debit Card Number • Electronic Protected Health Information-HIPAA • FERPA-protected data • Gramm Leach Bliley data and other data protected by law or regulation • Passport Number • DOD contracted “Applied Research” • Electronic Credentials (PINs, Passwords, Tokens, etc.) • Law Enforcement Active Investigation Data **Declared Data** • System Administrator/ Net ID Authentication Credentials • Documents protected by Attorney Client Privilege These examples are not an exhaustive list of this classification’s data.

Data Classification	Risk from Disclosure	Description	Examples
Category II: Internal Use Data	Medium-Low	Category II includes non-public, internal use information that is not subject to state or federally mandated protections. This includes data exempt from disclosure in NY State's Freedom of Information Law (FOIL), as well as information that would normally require a FOIL request for public release.	• Other HR Employment Data • Law Enforcement Post Investigation Data • Public Safety Information • IT Infrastructure Data • Collective Bargaining/Contract Negotiation Data • Trade Secret Data • Protected Data Related to Research • College Intellectual Property • College Proprietary Data • Data protected by non-disclosure agreements • College Financial Data • Cortland/Employee ID • Meeting Minutes • Administrative process data • Data about decisions that affect the public • Licensed Software • Inter- or Intra-Agency Data which are **not**: statistical or factual tabulations; instructions to staff that affect the public; final agency policy or determination; external audit data (See Appendix) These examples are not an exhaustive list of this classification's data.
Category III: Public Data	None	All public data	• General access data, such as that on unauthenticated portions of cortland.edu

Information Security Roles and Responsibilities

Data Classification Steering Committee

The Data Classification Steering Committee will be responsible for reviewing and updating (if necessary) the Data Classification Standards and Policy annually. This committee shall be composed of the Associate Provost for Information Resources, the Information Security Officer, the Director of Systems Administration and Web Services, the Director of Networking and Telecommunications, and the Risk and Compliance Officer.

Information Security Team

The Information Security Team will approve how Institutional Data is stored, processed and transmitted by the College and by third-party Agents of the College. This can be accomplished through review of data flow documentation maintained by a Data Custodian. In situations where Institutional Data is being managed by a third-party, the contract or service level agreement should require documentation of how data is or will be stored, processed and transmitted. The Information Security Team is composed of the Associate Provost for Information Resources, the Information Security Officer, the Director of Systems Administration and Web Services, and the Director of Networking and Telecommunications.

Data Steward

A Data Steward is a senior-level employee of the College who oversees the lifecycle of one or more sets of Institutional Data. Responsibilities of a Data Steward include the following:

Assigning an appropriate classification to Institutional Data.

All Institutional Data should be classified based on its sensitivity, value and criticality to the College.

Assigning day-to-day administrative and operational responsibilities for Institutional Data to one or more Data Custodians.

Data Stewards may assign administrative and operational responsibility to specific employees or groups of employees. A Data Steward could also serve as a Data Custodian. In some situations, multiple groups will share Data Custodian responsibilities. If multiple groups share responsibilities, the Data Steward should understand what functions are performed by what group.

Approving operating procedures related to day-to-day administrative and operational management of Institutional Data.

While it is the responsibility of the Data Custodian to develop and implement operational procedures, it is the Data Steward's responsibility to review and approve these operational procedures. A Data Steward should consider the classification of the data and associated risk tolerance when reviewing and approving these procedures. For example, high risk and/or highly sensitive data may warrant more comprehensive documentation and, similarly, a more formal review and approval process. A Data Steward should also consider his or her relationship with the Data Custodian(s). For example, different review and approval processes may be appropriate based on the reporting relationship of the Data Custodian(s).

Determining the appropriate criteria for obtaining access to Institutional Data.

A Data Steward is accountable for who has access to Institutional Data. This does not imply that a Data Steward is responsible for day-to-day provisioning of access. Provisioning access is the responsibility of a Data Custodian in conjunction with Information Resources. A Data Steward may decide to review and authorize each access request individually or a Data Steward may define a set of rules that determine who is eligible for access based on business function, support role, etc. For example, a simple rule may be that all students are permitted access to their own transcripts or all staff members are permitted access to their own health benefits information. These rules should be documented in a manner that allows little or no room for interpretation by a Data Custodian. If no rule is present for a data set, the data custodian must consult the steward of the data before granting access or releasing data.

Understanding how Institutional Data is stored, processed and transmitted by the College and by third-party Agents of the College.

While the Information Security Team is responsible for approving how Institutional Data is stored, processed and transmitted, it is important for the Data Steward to understand these important standards in order to ensure reasonable and appropriate security controls are implemented. This can be accomplished through review of data flow documentation maintained by a Data Custodian. In situations where Institutional Data is being managed by a third-party, the contract or service level agreement should require documentation of how data is or will be stored, processed and transmitted.

Defining risk tolerance and accepting or rejecting risk related to security threats that impact the confidentiality, integrity and availability of Institutional Data.

Information security requires a balance between security, usability and available resources. Risk management plays an important role in establishing this balance. Understanding what classifications of data are being stored, processed and transmitted will allow Data Stewards to better assess risks. Understanding legal obligations and the cost of non-compliance will also play a role in this decision making. Both the Information Security Team and the Office of General Counsel can assist Data Stewards in understanding risks and weighing options related to data protection.

Understanding how Institutional Data is governed by College policies, state and federal regulations, contracts and other legal binding agreements.

Data Stewards should understand whether or not any College policies govern their Institutional Data. Data Stewards are responsible for having a general understanding of legal and contractual obligations surrounding Institutional Data. For example, the Family Educational Rights and Privacy Act (“FERPA”) dictates requirements related to the handling of student information. The Office of General Counsel can assist Data Stewards in gaining a better understanding of legal obligations.

Data Stewards are listed by area in Appendix B

Data Custodian

A Data Custodian is an employee of the College who has administrative and/or operational responsibility over Institutional Data. In many cases, there will be multiple Data Custodians. An enterprise application may have teams of Data Custodians, each responsible for varying functions. SUNY Cortland's FERPA Policy defines data custodians in accordance with student records. A Data Custodian is responsible for the following:

Understanding and reporting on how Institutional Data is stored, processed and transmitted by the College and by third-party agents of the College.

Understanding and documenting how Institutional Data is being stored, processed and transmitted is the first step toward safeguarding that data. Without this knowledge, it is difficult to implement or validate safeguards in an effective manner. One method of performing this assessment is to create a data flow diagram for a subset of data that illustrates the system(s) storing the data, how the data is being processed and how the data traverses the network. Data flow diagrams can also illustrate security controls as they are implemented. Regardless of approach, documentation should exist and be made available to the appropriate Data Steward. Transmitting, storing and processing of data should be in conjunction with Information Resources.

Implementing appropriate physical and technical safeguards to protect the confidentiality, integrity and availability of Institutional Data.

Information Resources has published guidance on implementing reasonable and appropriate security controls for three classifications of data: public, internal use and protected. See the Cortland Data Classification Standards for more information. Contractual obligations, regulatory requirements and industry standards also play in important role in implementing appropriate safeguards. Data Custodians should work with Data Stewards to gain a better understanding of these requirements. Data Custodians should also document what security controls have been implemented and where gaps exist in current controls. This documentation should be made available to the appropriate Data Steward.

*Please refer to the companion matrix to determine appropriate methods to transmit and store data.

Documenting and disseminating administrative and operational procedures to ensure consistent storage, processing and transmission of Institutional Data.

Documenting administrative and operational procedures goes hand in hand with understanding how data is stored, processed and transmitted. Data Custodians should document as many repeatable processes as possible. This will help ensure that Institutional Data is handled in a consistent manner. This will also help ensure that safeguards are being effectively leveraged.

Provisioning and de-provisioning access to Institutional Data as authorized by the Data Steward.

Data Custodians are responsible for provisioning and de-provisioning access based on criteria established by the appropriate Data Steward. As specified above, standard procedures for provisioning and de-provisioning access should be documented and made available to the appropriate Data Steward.

Understanding and reporting on security risks and how they impact the confidentiality, integrity and availability of Institutional Data.

Data Custodians should have a thorough understanding of security risks impacting their Institutional Data. For example, storing or transmitting sensitive data in an unencrypted form is a security risk. Protecting access to data using a weak password and/or not patching a vulnerability in a system or application are both examples of security risks. Security risks should be documented and reviewed with the appropriate Data Steward so that he or she can determine whether greater resources need to be devoted to mitigating these risks. The Information Security Team can assist Data Custodians with gaining a better understanding of their security risks.

Data Custodians are listed by area in Appendix C

Data Users

A Data User is a person that has been authorized access to specific data. Data Users are required to abide by all data classification rules defined by this policy and the Data Custodian.

In the Event of a Breach

If a Data Steward, Data Custodian or Data User discovers a security breach of any kind, immediately report it to the Help Center: phone (607) 753-2500. The Information Security Team will take immediate action to mitigate the breach, and begin forensic discovery to determine its cause.

Violation of this Policy

Violations of this policy may result in the immediate suspension and/or revocation of information technology resources privileges. Students may also be subject to disciplinary action in accordance with the Code of Student Conduct, and employees may also be subject to disciplinary action in accordance with appropriate Agreements between the State of New York and the various bargaining units. Violations of state and/or federal laws in the use of the College's data may also result in criminal prosecution of the individual student/employee and/or civil liability for the individual student/employee.

To report violations or request further information, please contact the Help Center at (607) 753-2500 or thc@cortland.edu.

Effective Date of this Policy

This policy will be effective July 1, 2016. By this date, training and resources will be in place to enable compliance with this policy.

Cabinet Approval: January 2016

APPENDIX A

RECORDS EXEMPTED FROM PUBLIC ACCESS (FOIL) – Taken from the NY State Department of Education, Office of the Chancellor Regulation[1]

A. The public has access to all records, except that the Department Of Education may deny access to records or portions of records that:

1. Are specifically exempted from disclosure by state or federal statute[2] (POL § 87(2) (a));
2. If disclosed, would constitute an unwarranted invasion of personal privacy (POL § 87(2) (b)) (see Section III below);
3. If disclosed, would impair present or imminent contract awards or collective bargaining negotiations (POL § 87(2) (c));
4. Are trade secrets or are submitted to an agency by a commercial enterprise or derived from information obtained from a commercial enterprise and which, if disclosed, would cause substantial injury to the competitive position of the subject enterprise (POL § 87(2) (d));
5. Are compiled for law enforcement purposes and which, if disclosed, would:
   a. interfere with law enforcement investigations or judicial proceedings;
   b. deprive a person of a right to a fair trial or impartial adjudication;
   c. identify a confidential source or disclose confidential information relating to a criminal investigation; or
   d. reveal criminal investigative techniques or procedures, except routine techniques and procedures (POL § 87(2) (e)).
6. If disclosed, would endanger the life or safety of any person (POL § 87(2) (f));
7. Are inter-agency or intra-agency materials unless they are:
   a. statistical or factual tabulations or data;
   b. instructions to staff that affect the public;
   c. final agency policy or determinations; or
   d. external audits, including but not limited to audits performed by the comptroller and the federal government (POL § 87(2) (g)).
8. Are examination questions or answers which are requested prior to the final administration of such questions (POL § 87(2) (h)); or
9. If disclosed, would jeopardize an agency's capacity to guarantee the security of its information technology assets, such assets encompassing both electronic information systems and infrastructures (POL § 87(2) (i)).

B. The release of and access to student records is governed by FERPA (the Family Educational Rights and Privacy Act, 20 U.S.C. 1232g). See Chancellor's Regulation A-820, *Student Records: Confidentiality, Access, Disclosure and Retention.* Generally, information that would tend to identify a student, including but not limited to his/her name, student identification number and parent's name, must be redacted from documents prior to their release. However, if the requester represents the parent or

[1] Complete regulation from the NY State Department of Education, Office of the Chancellor is available at: http://docs.nycenet.edu/docushare/dsweb/Get/Document-84/D-110 1-9-03.pdf

[2] For example, FERPA, the Family Educational Rights and Privacy Act, 20 U.S.C. 1232g.

eligible student whose record he/she is requesting and provides a written consent or release, the personally identifying information for his/her client will not be redacted.

Appendix B

Data Stewards by area

Data Type	Role	Name
Alumni/Donor Data	VP, Institutional Advancement	Peter Perkins
Academic Records	Provost	Mark Prus
Authentication Verifiers	CIO	Amy Berg
Covered Financial Information	VP, Finance	David Duryea
Electronic Protected Health Information (EPHI)/Counseling Services **Communication Sciences and Disorders**	Student Health Services: VP, Student Affairs Academic Department: Provost	Greg Sharer Mark Prus
Financial Aid Records	Provost	Mark Prus
Facilities Information and Drawings	VP, Finance	David Duryea
Payment Card Information	VP, Finance	David Duryea
Personally Identifiable Information	**Students**: Provost **Faculty & Staff**: VP, Finance	**Students**: Mark Prus **Faculty & Staff**: David Duryea
Police Records/Surveillance Data	VP, Student Affairs	Greg Sharer
Sponsored Research	Provost	Mark Prus

Appendix C

SUNY Cortland Data Custodians by area:

Educational Records and FERPA define custodians for specific subsets of an education record. Those custodians may be references via the web at http://www2.cortland.edu/information/policies/ferpa/appendix.dot

Data Type	**Title**	**Department**
Department Records	Dean's Office	Various
Admissions "Pre-student" Data	AVP, Enrollment Management	Admissions
Alumni Records	Database Administrator	Alumni Engagement
Authentication Credentials	Director	Systems Admin. & Web Services
Career Services Credentials	Director	Career Services
Counseling Center	Director	Counseling Center
Degree Audit	Registrar	
Faculty & Staff PII	Human Resources Registrar	Various
Financial Aid Parent & Student Data	Director	Financial Aid
Financial Contracts **Construction Contracts**	Director Asst Director of Administration	Purchasing Facilities Planning, Design and Construction Office
Facilities Plans and Data	AVP	Facilities Management & Planning
Health Records	Director	Student Health Services
Payroll Data, Student, Faculty and Staff	Payroll Manager	Payroll
Parking/Vehicle Records	Chief of Police	University Police
Police Records	Chief of Police	University Police
Camera Surveillance Footage	Director, Campus Security Systems	University Police
Recreational Sports Systems **-Intramural/Club** **-SLC** **-Registration/Attendees**	Director	Recreational Sports
Center for Speech, Language and Hearing Disorders Clinic	Department Chair	Center for Speech, Language and Hearing Disorders

Networking Infrastructure Plans	Director	Networking and Telecommunications
Athletic: *Team Participation* *Attendee Information*	Director	Athletics
Campus Calendar	Project Coordinator	Information Resources
Building Management Systems	Energy Coordinator	Facilities
HelpSpot, Incident Tracking System	Associate Director, The Help Center	Memorial Library
Patron records (Library)	Associate Director	Memorial Library
Source Code (Software Applications)	Director(s)	Administrative Computing Systems Administration and Web Services
Personnel Data	AVP	Human Resources/Provost's Office
Call Detail Records	Director	Networking and Telecommunications
Search Committee Records	Affirmative Action Officer	Human Resources
Physical Space Inventory	Director	Facilities Management
Property Inventory	Property Control Officer	Purchasing
Foundation/Giving Records	Financial Operations	Advancement
Title IX	Title IX Coordinator	President's Office

Appendix D

These standards apply to the following data types only. Their distinguishing feature is that they are subject to federal, state, or local regulations, or declared sensitive and personally identifiable Category I data by SUNY Cortland.

	Approved or Recommended Storage Locations				Higher Risk or Prohibited Storage Locations				
	SUNY Cortland Hosted Services	SUNY Cortland IR Approved Cloud Services			SUNY Cortland Devices			Personal Device or Account (i.e., no formal agreement with SUNY Cortland)	
	Examples: Active Directory Windows Shares, Certified[1] Departmental Servers, Banner, OnBase	SUNY Cortland Email, Calendar Services and OneDrive for Business, Skype for Business		Hosted Services with Properly Reviewed and Executed Contracts	SUNY Cortland Owned and Supported Workstations & Laptops [8]	SUNY Cortland Owned Smart Phones & Tablets	Thumb/ USB/ Portable Hard drives	Personally owned device (e.g., home computer, smartphone, tablet, laptop, portable [USB, thumb] drives)[2]	Personally maintained services (e.g., Dropbox, OneDrive [OneDrive], Gmail, Google Drive, SurveyMonkey)[2]
Data Type		Sent or Shared Internally	Sent or Shared Externally						
A. Student Educational Records (FERPA)	Yes	Yes	No[4]	Yes	No	No	No	No	No
B. Protected Health Information (PHI-HIPAA)	Yes	Must be Encrypted Prior to Transmission	No	Must be Encrypted Prior to Storage	No	No	No	No	No

C. Personally Identifiable Information per NYS Information Security Breach Notification Act (i.e., Names + SSNs or DMV # or Financial Account #)	Yes	Yes	Must be Encrypted Prior to Transmission	Must be Encrypted Prior to Storage	No	No	No	No	No
D. Declared Category I data (Banner and System Administrator authentication credentials, attorney/client privilege documents, passport numbers).	Yes	Must be Encrypted Prior to Transmission	Must be Encrypted Prior to Transmission	Must be Encrypted Prior to Storage	No	No	No	No	No
E. HR Data: not PHI, not SSNs, not payroll; otherwise see C.	Yes	Yes	Yes	Yes	Password Protected[5]	Password Protected[5]	No	Password Protected[5]	No
F. Gramm Leach Bliley (GLBA) e.g., student loan, financial aid data: not SSNs, not financial account #s; otherwise see C.	Yes	Yes	Yes	Yes	Password Protected[5]	Password Protected[5]	No	Password Protected[5]	No

G. Human Subjects Research	Yes	Conditional[6]	Conditional[6]	Conditional[6]	Password Protected[5]	Password Protected[5]	No	Conditional[6]	Conditional[6]
PCI – Credit Card Information	No	No	No	No	No	No	No	No	No

[1] Servers that are in compliance with SUNY Cortland's Standards for Connecting Servers to the University Network, are known to and supported by IR.

[2] Storing College business records within personally owned or maintained storage services exposes the institution to additional risk with respect to e-discovery, security breaches, and data retention and recovery. Furthermore, SUNY Cortland exerts a claim of ownership over business records saved on personally maintained devices or sites.

[3] Internal correspondence (cortland.edu-to-cortland.edu) is encrypted in transit. However, personally identifiable or health information should be sent as encrypted attachments to prevent exposure in the event the recipient has their mail forwarded to a non-cortland.edu account.

[4] FERPA correspondence with students is limited to cortland.edu accounts. Sharing is limited to properly contracted partners.

[5] Mobile/portable devices must be password protected and reported when missing. For additional security recommendations, please see http://www.fcc.gov/smartphone-security.

[6] Subject to Office of Regulatory Research Compliance (ORRC) and/or Institutional Review Board (IRB) determination of compliance with applicable regulations, sponsor requirements, data use agreements, and SUNY Cortland policies which might impose additional obligations and requirements.

[7] Export Controlled Research is highly regulated. Sanctions for violations can include criminal charges. PIs are urged to carefully review and comply with the terms and conditions of their research contracts.

[8] Services which provide syncing to supported cloud based services should be classified as desktop application and placed in the appropriate storage locations

Appendix E

These standards apply to the following data types only, includes non-public, internal use information that is not subject to state or federally mandated protections. This includes data exempt from disclosure in NY State's Freedom of Information Law (FOIL), as well as information that would normally require a FOIL request for public release.

	Approved or Recommended Storage Locations				Higher Risk or Prohibited Storage Locations				
	SUNY Cortland Hosted Services	SUNY Cortland IR Approved Cloud Services			SUNY Cortland Devices			Personal Device or Account (i.e., no formal agreement with SUNY Cortland)	
	Examples: Active Directory Windows Shares, Certified1 Depart-mental Servers, Banner, OnBase	SUNY Cortland Email, Calendar Services and OneDrive for Business, Skype for Business		Hosted Services with Properly Reviewed and Executed Contracts	SUNY Cortland Owned and Supported Work-stations & Laptops 8	SUNY Cortland Owned Smart Phones & Tablets	Thumb/ USB/ Portable Hard drives	Personally owned device (e.g., home computer, smart phone, tablet, laptop, portable [USB, thumb] drives)2	Personally maintained services (e.g., Dropbox, OneDrive [OneDrive] Gmail, Google Drive, Survey Monkey)2
Data Type		Sent or Shared Internally	Sent or Shared Externally						
A. Collective Bargaining/Contract Negotiation Data	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No

B. IT Infrastructure Data	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
C. University Financial Data	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No
D. SUNY Cortland C-Number	Yes	Yes	Must be Encrypted Prior to Transmission	Must be Encrypted Prior to Storage	Yes	No	Yes	No	No
E. Meeting Minutes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
F. Public Safety Information	Yes	Yes	Yes	Yes	Password Protected[5]	Password Protected[5]	No	Password Protected[5]	No
G. Post Law Enforcement Investigation Data	Yes	Conditional[6]	Conditional[6]	Conditional[6]	No	No	No	No	No
Licensed Software	Yes	Yes	No	Yes	Yes	Yes	Yes	Conditional	Conditional
Data protected by non-disclosure agreements	Yes	Yes	Conditional	Conditional	Yes	Yes	No	No	No
Protected Data Related to Research	Yes	Yes	Conditional	Yes	Yes	Yes	Yes	Conditional on DMP	Conditional on DMP
Trade Secret Data	Yes	Yes	No	Yes	Yes	Yes	No	No	No
