CATHERINE CUTLER INSTITUTE

Protected Information Policies and Procedures

Last revised: August 2024

If you have any questions about Protected Information, or about how these Policies and Procedures apply to your work, please contact Cutler's Compliance Coordinator.

Contents

A. The Basics

1) What is the Purpose of this Policy?

The purpose of this policy is to ensure that all Catherine Cutler Institute personnel, and those acting on the Institute's behalf use and secure information within the University environment in compliance with the highest legal and ethical standards whenever that information is legally protected under a statute, regulation, contract, or research protocol, or when it otherwise merits protection because it is sensitive, private, or proprietary.

2) Who Needs to Comply with this Policy?

This policy applies to all Catherine Cutler Institute employees, contractors, students, temporary staff, and any other individual employed by or under contract to the University (i.e., agents of the University) who access or possess **Protected Information** associated with a research, training, or technical assistance project under the direction of a **Principal Investigator** within the Catherine Cutler Institute, as those terms are defined in this policy.

In addition, this policy requires all Catherine Cutler Institute personnel and those acting on the Institute's behalf to safeguard any Protected Information collected for any purpose (*e.g*., social security numbers, student IDs, or other personal identifiers collected for administrative purposes) in compliance with Part B.

If this Policy applies to any individual who is obligated by contract or other legal authority to follow stricter procedures relating to Protected Information, that individual shall follow the stricter procedures. For example, a contract may include additional reporting or documentation requirements that go beyond the requirements set forth in this Policy If this Policy applies to anyone who is subject to conflicting requirements related to Protected Information by contract or other legal authority, the individual should consult with the Principal Investigator and/or the Compliance Coordinator.

3) How does this Policy Relate to Other University Policy?

This policy is written in the context of applicable University of Maine System (UMS) and University of Southern Maine (USM) policies and procedures, including:

- Information Security policies maintained by the University of Maine System's Chief Information Security Officer located at: https://www.maine.edu/information-technology/security-privacy/
- University of Maine System Health Insurance Portability and Accountability Act (HIPAA) Policies and Forms: https://www.maine.edu/general-counsel/university-of-maine-system-hipaa-policies-forms/

This policy is designed to guide Catherine Cutler Institute employees and agents on how to comply with UMS, USM and other applicable standards (*e.g.*, standards under a Business Associate Agreement, Data Use Agreement, or IRB protocol) within the context of the

Catherine Cutler Institute and University environments. This policy does not supersede, replace, modify, or limit applicable UMS or USM policies and procedures, ***except where this policy is more stringent.***

This policy also complements UMS and USM policies and procedures, as referenced elsewhere within this document, so that, together, all three sets of policies and programs implement the requirements of HIPAA within the context of the Catherine Cutler Institute and university environment.

4) How does this Policy Relate to IRB Requirements?

The Office of Research Integrity and Outreach (ORIO) and the Institutional Review Board (IRB) are responsible for overseeing "research" as that term is defined under federal law. Only ORIO can determine if a project meets the definition**.** Human Subjects Research often involves acquiring, collecting, or creating information that is Protected Information.

This policy governs any Protected Information governed under an IRB-approved research protocol. However, not all Protected Information is governed by IRB requirements. Data Use Agreements (DUA) and Business Associate Agreements (BAA) may also apply.

5) What Are My Responsibilities Under this Policy?

Every Catherine Cutler Institute employee has some basic level of responsibility for Protected Information within our university environment under this policy. This is the case whether or not you are directly working with Protected Information. Depending on your role(s), you may have additional responsibilities to those listed below. Responsibilities are described more fully in later sections of this policy.

a) **All Institute Employees.** All Catherine Cutler Institute employees are responsible for:

  i. Completion of all required USM compliance training, including successful completion of the CITI Health Information Privacy and Security (HIPS) for Researchers **by December 31st annually.**

  ii. Complying with the Federal and State regulations, UMS, USM's IRB, and Catherine Cutler Institute's policies for reporting adverse events. These responsibilities are described in greater detail in Section B.

  iii. Being able to spot Protected Information;

  iv. Acquiring, Using and Disclosing Protected Information only as Permitted or Authorized;

  v. Acquiring, Using and Disclosing only the Minimum Necessary Protected Information;

  vi. Safeguarding Protected Information in compliance with UMS, USM and these policies and procedures; and

b) **Principal Investigator.** For the purpose of this policy, the Principal Investigator is the person recognized as the single point of accountability for an externally- funded project by the Grant Administration Service Center. In some situations, this may include University-funded projects; the Principal Investigator may or may not be the same individual serving as Project Director (See paragraph c) below). In addition to any other responsibility identified under this policy, the Principal Investigator is responsible for, with respect to any Protected Information associated with his or her project(s):

i. Acquiring, creating, using, disclosing, handling, and securing the Protected Information consistent with applicable law, contracts, IRB-approved research protocols, and University policy; (A Principal Investigator has responsibility for ensuring compliance with an IRB-approved research protocol in coordination with the Project Director of the Project Director is a different individual);

ii. Maintaining up-to-date documentation for all Protected Information associated with a project, including ensuring data is accurate in PIMS and kept up to date and that project extensions are properly documented;

iii. Ensuring contracts and subcontracts address the use and disclosure of Protected Information, when applicable;

iv. Ensuring that project budgets and timelines reflect any additional costs and tasks associated with the Protected Information;

v. Ensuring project staff have completed required compliance training annually and understand their responsibilities in using or handling Protected Information;

vi. Reporting and responding to adverse events associated with the project; and

vii. Work with Cutler's Technology Manager on the destruction of protected information, including proper documentation, of all project data with Protected Information in accordance with funder requirements and compliance with the applicable data destruction procedure(s) outlined in Section B.4.

While a Principal Investigator may delegate the performance of one or more of these tasks to a Project Director, the Principal Investigator retains responsibility for ensuring the performance of these tasks. These responsibilities are described in greater detail in Section C.

c) **Project Directors**. For the purpose of this policy, a Project Director is a university employee acting on behalf of the Principal Investigator or co-Principal Investigator under a research protocol approved by the University's Institutional Review Board. In addition to any other responsibilities under this policy, the Project Director is responsible for ensuring that all members of the research team (including students, business partners, contractors, and consultants) understand their roles and responsibilities regarding Protected Information governed under the research protocol.

d) **Data Custodians**. For the purpose of this policy, a Data Custodian is a university employee acting on behalf of the Principal Investigator or Project Director who is granted administrative rights to Raw Data and/or Protected Information with Direct Identifiers for 500 or more individuals associated with an externally funded project or an IRB-approved research protocol. Within Cutler the Data Custodian is the PI, PD, or SQL Database administrator assigned to the project.

e) **Supervisors**. As applicable, the Supervisor has responsibility for ensuring that all supervised employees are educated about their responsibilities for Protected Information, addressing performance improvement and sanctions, as applicable, and complying with other responsibilities more fully described in Section **B, For All Catherine Cutler Institute Employees**.

f) **Compliance Coordinator.** The Compliance Coordinator (see contact information in Appendix) provides regulatory and administrative support to projects involving, or potentially involving, protected information at the Catherine Cutler Institute. See the Appendix for contact information.

g) **The Office of Research Integrity and Outreach (ORIO).** ORIO oversees the state, federal and local compliance regulations for human subject research. ORIO is responsible for the Institutional Review Board (IRB). The Compliance Coordinator works with ORIO in reference to human subject research and compliance with above referenced regulations. ORIO reviews and creates best practices for ensuring adherence to policies and procedures regarding the safe use and handling of protected information by researchers within the Catherine Cutler Institute.

h) **Cutler Institute Technology Manager.** The Technology Manager (see contact information in Appendix) is responsible for:

i. Reviews data authorization details provided by IRB Protocol, DUA, MOU, BAA, or other contractual agreement;
ii. PIMS Administration, including data entry input into the Protected Information Management System (PIMS);
iii. Provides, records, and/or coordinates compliant resources, access, and data destruction;
iv. Acts as the liaison to University System IT to coordinate solutions for compliant research or specific project needs;
v. Regularly communicates with PIs/PDs regarding user access, data destruction, and compliant project review reminders;
vi. Provides Cutler-wide reporting to IMT, University IT, ORIO, and others upon requests as required and appropriate;
vii. Certifies and/or coordinates data destruction certification;
viii. Provides and/or coordinates hardware and software quotes upon request as appropriate;
ix. Annually provides compliant process training and on-demand training for new PIs, PDs, and Data Custodians;
x. Ensures temporary and student staff requiring compliant access have been assigned the Basic Cutler HIPS CITI Training and that it is completed before compliant access is granted; and
xi. Documents exceptions to the policy as appropriate and necessary in collaboration with the Compliance Coordinator.
xii. Makes recommendations and escalates compliance concerns to IMT.

i) **Catherine Cutler Institute Director and Integrated Management Team**. The Director and the Integrated Management Team are responsible for:

i. Approves and enforcing this policy and related procedures;

ii. Allocates resources as necessary to support risk analyses, compliance evaluations, monitoring and tracking of compliance, training, and other activities necessary to support compliance with this policy;

iii. Accepts reports on performance and responding to recommendations for improvement from the Compliance Coordinator, as listed in Section E, Resources, and updated from time to time;

iv. As appropriate, referring an employee's or student's violation of this policy to the employee's supervisor, Institutional Review Board (if applicable), or the University's Conduct Officer for appropriate action

B. For All Catherine Cutler Institute Employees

1) How do I Spot Protected Information?

a) **What is Protected Information?** Information is Protected Information when it is:

i. **Legally Protected.** Legally Protected Information is any information that the University has a legal responsibility to protect, such as information that must comply with regulations. That responsibility might be defined under a:

(1) **Federal or state statute or regulation.** Many Cutler Institute employees think of the Health Insurance Portability and Accountability Act (HIPAA) when they think of Protected Information which governs the use of Protected Health Information (PHI). However, there are many laws that place protections around different types of information, including federal (e.g., the Family Educational Rights and Privacy Act (FERPA) which governs student records, or federal regulations, which govern the confidentiality of substance abuse treatment records) and state statutes (governing, for example, the disclosure of HIV status or the confidentiality of records created in connection to child or adult protective services).

(2) **A contract**. For example, the contract might authorize the university to use Protected Information (PHI or PI) for which the other entity has legal responsibility, or the contract might authorize the university to compile Protected Information on the other entity's behalf.

(3) **Research protocol approved by the University's Institutional Review Board.** When you submit a research protocol, you make a commitment to safeguard the Protected Information you use or create in accordance with the terms of the research protocol. Once approved, you must comply with the terms of

your approved protocol.

ii. **University policy**. Under the University of Maine System policy, this category of Protected Information meets the definition of “Restricted Data” or “Confidential Data.” Stringent or prescribed requirements exist for these kinds of data, including special permissions, training, hardware, software, and incident response. Restricted confidential data should be used only when no alternative exists and must be carefully protected. Any unauthorized access, use, disclosure, modification, or loss or destruction of Restricted or Confidential data must be reported and in accordance with regulation, statute, contract, University policy, and any other requirement or agreement. More information about these data classifications can be found at APL VI-I.

b) **Sensitive information.** This is information not subject to statutory or contractual controls but is information that is not intended to be readily available to the public but for which a compromise of its confidentiality, integrity or availability could result in damage or loss to UMS. This category might include proprietary information belonging to the University (*e.g.,* research or data analytic methods that we have developed) or market strategies. The University of Maine System policy calls this category of information “Internal.” In addition, Cutler Institute Policy includes “private” information – information that is not legally protected, but for which the person providing the information could reasonably expect that it is not disclosed. This policy provides guidelines for the use and disclosure of sensitive information.

c) **Is There a Difference Between Individually Identifiable Information and Protected Information?** Individually Identifiable Information includes a Direct Identifier or an Indirect Identifier. Not all Individually Identifiable Information is Protected Information (*e.g.*, the names and addresses listed in a phone book), and not all Protected Information is Individually Identifiable (*e.g.*, proprietary information about business strategy or practices). Information is only Protected Information when it is Legally Protected or Sensitive (see above).

TIP: Individually Identifiable Information Is Not Always Protected Information

Protected Information: Name and address in medical record.

Not Protected Information: Name and address in phone book.

TIP: Non-Individually Identifiable Information May Be Protected Information

Examples:

- *Our own intellectual property.*
- *Information we are required to protect under a contract (e.g., someone else's intellectual property under a licensing agreement).*

i. **Why is it Important to know when information is Individually Identifiable?** We need to know when information is Individually Identifiable because many laws protecting information apply only to Individually Identifiable Information. In those cases, we need to know when information has been De-Identified so, we know when that information is no longer Protected Information.

ii. **What Is De-Identified Information?** Under our policy, Individually Identifiable Information includes Direct or Indirect Identifiers, consistent with the requirements under HIPAA. De-identified information is information with those identifiers removed.

(1) **Direct Identifiers.** Direct Identifiers include *any uniquely identifying number*, *characteristic, or code*, including:

- Names
- Postal address information, other than town or city, state, and zip code
- Telephone numbers
- Fax numbers
- Electronic mail addresses;
- Social security numbers;
- Medical record numbers;
- Health plan beneficiary numbers;
- Account numbers;
- Certificate/license numbers;
- Vehicle identifiers and serial numbers, including license plate numbers;
- Medical device identifiers and serial numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) addresses;
- Biometric identifiers, including finger and voice prints;
- Full face photographic images and any comparable images; and
- Any other unique identifying number, characteristic, or code.

(2) **Indirect Identifiers.** Indirect Identifiers include any information for which there is a *reasonable basis to believe it can be used alone or in combination with other information to identify an individual*, including but not limited to:

- Town, city, or zip code; and

- All elements of dates (except year) directly related to an individual, including birth date, admission date, discharge date, date of death, and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older.

(3) **De-Identified Information.** De-identified information is information that has no Direct Identifiers or Indirect Identifiers.

TIP: "Reasonable Basis" and Indirectly Identifiable Information

The examples below illustrate some of the things you want to think about when you are trying to decide whether there might be a "reasonable basis" for determining that information without identifiers can be used to identify an individual.

Combining Multiple Sources of Data: You are producing two different data sets, using data for the same group of people. In one, you've eliminated everyone who has a behavioral health condition, substance use disorder, or positive HIV status. In the other, you've eliminated any information about the behavioral health condition, substance use disorder or HIV status, but you've kept everyone in the data set, including those you deleted in the other data set. A person who knows the difference between the two data sets can identify, through a process of elimination who might have one of those three conditions.

Small Cell Size: You are examining chronic health conditions in rural Maine and discover that only 10 people in Cherryfield are both female and HIV positive. Is there a "reasonable basis" for determining whether that information can be used, alone or in combination with other information, to identify an individual? Some Data Use Agreements (*e.g.*, those governing Medicaid and Medicare data) define "de-identified" to be data presented in table form, with cell sizes smaller than 11 suppressed (*i.e.*, no value is presented in that cell). In general, suppressing small cell sizes is a good safeguard even if it's not required by your data use agreement.

d) **What is Protected Health Information?** Protected Health Information (PHI) is a particular type of Protected Information defined under HIPAA.

i. **Protected Health Information**:

(1) Includes Direct or Indirect identifiers;

(2) Is created or received by a Covered Entity or a Business Associate acting on behalf of a Covered Entity; and

(3) 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.

ii. **Covered Entity:** A Covered Entity is a Health Plan, a Health Care Provider, or a Health Care Clearinghouse. Large complex organizations may include some organizational units that qualify as a Covered Entity (called "Covered Components") and some organizational units that are not covered under HIPAA. These organizations are called "hybrids." For example, the Maine Department of Health and Human Services is a hybrid organization with several units qualifying as a Covered Entity and others not.

(1) **Health Plan:** A Health Plan is an individual or group plan that provides or pays the cost of medical care. A health plan may include an employer-sponsored plan. The Medicaid program, the State Child Health Program (SCHIP), and other government-funded health plans are covered under HIPAA.

(2) **Healthcare Care Provider: A Health Care Provider is any person or organization that furnishes, bills, or pays for Health Care and** also electronically transmits health information in connection with certain transactions (*e.g.*, claims, benefits eligibility inquiries, authorization requests). Providers who use a third party to perform these transactions are also included. An individual can be a Covered Entity if the individual meets all the criteria, including electronically transmitting health information in connection with certain transactions. Under certain circumstances, a Health Care Provider under HIPAA may include providers of employment services, homemaker services, case management, or other services not traditionally thought of as health care.

(3) **Health Care:** Health Care includes preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service assessment, or procedure with respect to the physical or mental condition or functional status of an individual or that affects the structure or function of the body.

(4) **Health Care Clearinghouse:** A health care clearinghouse processes nonstandard information received from another entity into a standard (*i.e.*, standard format and content), or vice versa. Examples include billing services or community health management information systems.

TIP: Health Information is Not PHI
Unless created by or on behalf of a Covered Entity

A Lot of Health Information but Not Protected. Your friend Sandy tells you about her brother-in-law Stan's double bypass. She mentions that Stan's doctor has told him he needs to lose 100 pounds, stop smoking and stop drinking so much beer. But Sandy thinks Stan won't be able to deal with these issues until he starts taking his medication for anxiety and depression.

Very Little Health Information but Protected. Your friend Alice mentions that she bumped into a mutual friend, Manny, the other day, while he was waiting to be admitted as a patient at the hospital where Alice works. She tells you it had been so many years since she last saw him, she almost walked by without recognizing him.

e) **What is a High-Risk Personal Identifier? The University refers to 10 M.R.S.A., Chapter 210-B Notice of Risk to Personal Data.** High-Risk Personal Identifiers are Direct Identifiers at high risk of identity theft. These High-Risk Direct Identifiers should not be used or disclosed unless necessary and only when authorized or permitted, as described below. These Identifiers are protected under federal and state law and include, at a minimum:

i. **Name and Identifier**. A person's first name or first initial and last name in combination with any one or more of the following, when either the name or the data elements are not encrypted or redacted:

(1) Social Security number;

(2) Driver's license or state identification card number;

(3) Account number, credit card number, or debit card number, if circumstances wherein such a number could be used without additional identifying information, access codes, or passwords;

(4) Account passwords or personal identification numbers or other access codes.

ii. **Combination of Identifiers.** Even when not connected to an individual's first name, first initial, and last name, any combination of the identifiers listed above is considered a High-Risk Identifier if the information taken together is sufficient to permit a person to fraudulently assume or attempt to assume the identity of the person's whose information was compromised.

iii. **Other Data Elements.** The University of Maine System has identified several other data elements classified as "Restricted Data" that require a high level of protection. These data elements should be treated as high-risk Identifiers. For more details, please visit Administrative Practice Letter VI-I- Data Classification.

2) When Can I Use or Disclose Protected Information?

a) What is the difference between a "Use" of Protected Information and a "Disclosure"?

i. A **Use** of Protected Information happens within the legal boundaries of the University. For example, a use occurs when a member of a project team analyzes Protected Information or when an administrative assistant submits a form to Business Services with someone's Social Security number or driver's license on it. A proper use is either permitted or authorized, as defined below.

ii. A **Disclosure** of Protected Information occurs across the legal boundaries of organizations when the organization holding the Protected Information divulges the information to another organization. For example, a disclosure occurs when a data analyst creates a data extract of Protected Information and sends it to a researcher at another university. A proper disclosure is either permitted or authorized, as defined below.

b) When is a Use or Disclosure Authorized or Permitted?

We can only *use* or *disclose* Protected Information when it is *authorized* or *permitted*.

i. **Authorized**. A use or disclosure is *authorized* when an individual allows the organization holding his or her Protected Information to use or disclose it. The elements of an authorization (sometimes called a "release" or "consent") may be specified under a law. For example, under HIPAA, authorization must meet very specific requirements. The entity legally responsible for the Protected Information is the entity that is responsible for making sure that the authorization complies with the law.

ii. **Permitted.** A use or disclosure is *permitted* when the use or disclosure is allowed under the applicable law, contract, IRB-approved research protocol, or any other legal terms governing the Protected Information.

c) How do I know if the Use or Disclosure of Protected Information is Authorized or Permitted?

The legal terms that permit a use or disclosure usually define:

i. The outer boundaries of the Protected Information that you may use or disclose;

ii. Who may use the Protected Information or to whom it may be disclosed; and

iii. The purpose for which the Protected Information may be used or disclosed. Protected Information may only be used or disclosed consistent with these terms.

d) What happens when a Use or Disclosure is not Authorized or Permitted? An unauthorized or impermissible use or disclosure is presumed to be a *breach* unless the University can show that there is a low probability that the Protected Information has been compromised. An employee who becomes aware of an adverse event that potentially involves the unauthorized or impermissible use or disclosure is required to immediately notify the project's Principal Investigator so they can report the adverse event consistent with the UMS and Cutler Institute's Event Reporting Protocol. Any staff member may also report an anonymous concern about an issue of non-compliance using the noncompliance web form.

See Section B. **[8]**, **What Do I Do When Things Go Wrong?** for more information about breaches and the Event Reporting Protocol.

3) What is the Minimum Necessary Protected Information?

Even when you are authorized or permitted to use or disclose Protected Information, you may only use the **Minimum Necessary** to achieve a **legitimate project objective**. This policy defines three main categories of Minimum Necessary Protected Information depending on the legitimate project objectives:

a) **Default.** The Minimum Necessary Information is de-identified information unless a legitimate project requires Direct Identifiers or Indirect Identifiers, as described below.

b) **Indirect Identifiers.** The Minimum Necessary Information may include Indirect Identifiers if the Principal Investigator determines that legitimate project objectives cannot be achieved without access to Indirect Identifiers. For example, you need zip codes to analyze geographic differences.

c) **Direct Identifiers.** The Minimum NecessaryInformation may include Direct Identifiers if the Principal Investigator determines that legitimate project objectives cannot be achieved without access to Direct Identifiers because:

i. Direct Identifiers are required to link data sets; or

ii. Direct Identifiers are required for data collection strategies used to achieve legitimate project objectives (*e.g.*, to recruit participants for or conduct a focus group, survey, or interview); or

iii. A Catherine Cutler Institute employee or agent is responsible for providing technical assistance to another entity; the Protected Information is in the possession or control of the other entity, and access to Direct Identifiers is necessary to accomplish legitimate project objectives connected to the technical assistance function.

TIP: "Minimum Necessary" May Be Different for Different Team Members

Members of a project team have different roles and are, therefore, likely to require different levels of access to Protected Information to complete their work on a project. A Principal Investigator is responsible for determining which team members need which level of access to Protected Information. For example, a programmer might be responsible for linking and de-identifying the data, but an analyst might only need to work with a limited data set after all Direct Identifiers have been removed. The analyst should not have access to the identifiable data.

4) How Do I Securely Handle Electronic Protected Information?

Electronic Protected Information is Protected Information that is transmitted by electronic media or maintained in electronic media. An electronic audio or video file recording a focus group or interview may contain Protected Information.

This policy is intended to complement UMS policy governing the security of electronic Protected Information by providing specific guidance on how UMS policies are to be implemented within the context of the Cutler Institute and University system environment.

a) How do I Securely Store Electronic Protected Information?

Electronic Protected Information held by the Cutler Institute may only be stored on an Approved Server or on an encrypted portable storage device, consistent with the requirements of this section.

i. **Approved Servers**. An Approved Server is a server approved for storing Legally Protected Information by UMS IT Services (US:IT). You may store Protected Information only on an Approved Server. To request storage on our compliant file and SQL servers, please complete the Compliance Resource Request webform.

Catherine Cutler Institute employees who work as contractors based in State of Maine offices are permitted to use state laptops as authorized by the State and may store Protected Information on State network servers behind the State firewall if approved by the State**. State data should never be transported or utilized within the university's environment without express permission to do so from the state**.

ii. **Electronic Devices.** You MAY NOT store electronic Protected Information on a local hard drive (e.g. a desktop or laptop computer). Consistent with the procedures defined under C.4., you may temporarily store Protected Information on an encrypted portable storage device (e.g. USB drive) for transportation or, if explicitly permitted by contract or DUA and deemed necessary by the PI to meet project deliverables, for longer term storage. In all such cases, the PI is responsible for complying with requirements of C.4 and ensuring the physical safeguarding of the encrypted portable storage device such as storing the device in a secure lockable cabinet. Make sure that only those persons authorized to access the Protected Information may have access to the office and lockable cabinet.

Please note: All encrypted USB's need to be certified with NIST FIPS Program Validation and meet FIPS 140-2 Level 3 validation. For a list of NIST validated encrypted devices approved for purchase, please contact Cutler's Technology Manager at Cutlertech@maine.edu.

b) How do I Securely Transmit Protected Information? You may transmit electronic Protected Information only when encrypted, whether through an encrypted portable device or through a secure file transfer system. Portable devices may only be utilized for the transportation of encrypted data and must be either sanitized or overwritten after the data has been transported. **Protecting a document with Protected Information with a password but not encryption is not a secure method of transmitting electronic Protected Information.** If you have questions about the adequacy of encryption, consult the Cutler Technology Manager.

i. The Cutler Institute provides SFTP secure file transfer. The SFTP service only accepts traffic from specified IP addresses so a request for use requires discovery and sharing the source IP address. This address will be associated with the request user, which may need to be modified over time depending on the end-users Internet Service Provider. The use of an FTP client is required, and we prefer users install FileZilla, which is free from the University Software Center. External staff can download and install it from the internet. Cutler has utilized a HIPAA classified Windows server 2019, which is updated and patched monthly. The server hosts Bitvise SSH software, which offers state-of-the art cryptographic protection comparable with TSL/SSL. The key feature is that data is encrypted during transmission. For PIs who need secure electronic file transfer for their projects, please complete the SFTP server request webform.

ii. Fax over IP (FoIP) via Xmedius server

iii. When allowed by contract or DUA, and/or if explicitly permitted in an IRB protocol, protected information may be shared using the HIPAA-compliant version of Zoom. All such use shall be in compliance with minimum necessary standards. To request this version of Zoom email Cutler's Technology Manager at CutlerTech@maine.edu. Protected information may not be shared using other web conferencing platforms.

c) **Can I transmit protected information electronically through email? Transmitting electronic Protected Information through the maine.edu email system DOES NOT meet the secure transmittal standards of this Policy, even when the transmittal is within the maine.edu email system.** When Protected Information is sent or received by email it is not possible to destroy the Protected Information. In the absence of its destruction, immediately delete the email from all folders (including Sent and Trash folders) and request its deletion by those receiving the email. For email attachments opened, contact Cutler's Technology Team for guidance on how to securely delete the file and employ a drive sanitization tool that securely deletes temporary files and free space. You can also follow the steps outlined in **What Do I Do When Things Go Wrong?**

d) **How do I Securely Destroy Electronic Protected Information?** Electronic Protected Information may only be destroyed as follows:

i. **Destroying Devices.** When it is necessary to destroy University equipment or storage devices *(e.g.,* a server, computer, CD-ROM, flash drive, or back-up tape) with electronic Protected Information stored on it, the following security protocol applies:

To coordinate the removal and/or destruction of equipment, please contact the Cutler Institute Technology Manager (See Section E, Resources).

The Technology Manager will utilize the National Institute of Standards and Technology (NIST) Special Publication SP800-88: Guidelines for Media Sanitization to review current approved methods of media sanitization. Devices are imaged or securely wiped. HIPAA Compliant servers have a 30-day backup and are no longer available for file restoration to project staff. The storage is fully overwritten after the 30-day backup expires. Upon destruction, the Technology Manager will update PIMS stating the destruction date, staff involved, and sanitization method.

ii. **Reusing Devices.** Before reusing a device that has been used to store electronic Protected Information, please contact Cutler's Technology Manager to ensure it is first sanitized.

iii. **Destroying Electronic Data.** Principal Investigator, in conjunction with the

Technology Manager, are responsible for ensuring the destruction of compliant data. The Technology Manager shall ensure destruction requirements are met and record the date of the data destruction in PIMS.

When the data destruction date for your project arrives, the Technology Manager will confirm with the PI that the data is no longer in use before data destruction. The data should only be retained if the project is in the process of a date extension or renewal, which would follow up with a new contract, DUA, or IRB project number. If an extension or renewal is in progress, then the Technology Manager will check in monthly with PI to review the next steps.

Upon data destruction, you will receive confirmation of your request and notification that the data has been destroyed. If the grant contract requires official data destruction documentation or has specific data destruction requirements, please let the Technology Manager know a week IN ADVANCE of the data destruction. Any created work product (devoid of Protected Information) should be stored with the general storage project files by the Principal Investigator or Project Director.

5) How Do I Securely Handle Paper Protected Information?

All employees take the following measures to prevent unauthorized access to Protected Information stored on paper:

a) **Storage.** Paper files containing Legally Protected Information must be stored in a locked file cabinet. Sensitive Information must be stored either in a locked file cabinet or in a locked office. Make sure that only those persons authorized to access the Protected Information may have access to the file cabinet keys.

b) **Use.** Make sure that Protected Information in paper format is placed face down or concealed when unauthorized persons are present. When an office or desk is left unattended, secure the Protected Information to prevent unauthorized access.

c) **Copying and Printing.** Secure printing can be conducted on UMS: IT-deployed Xerox multi-function printers. Using this method, print jobs are securely transmitted to a secure PaperCut print server and then printed only when the user's campus card is presented at a Xerox printer. The print content is not stored on the printer. A printer connected directly to the computer (i.e., through USB, SCSI, Firewire, parallel port, or similar non-networked connection) is also permitted.

d) **Scans.** Employees may not scan Protected Information from paper to an electronic format in an area readily accessible by the public. Use a scanner and desktop computer in a secure area and scan the document to a secure location or folder as defined in Section B.4. Employees may not scan Protected Information to a shared drive or common folder.

e) **Transmittal**. You may transmit Protected Information in paper format through the mail or by hand carrier:

i. **Mail**. Send the Protected Information documents in a sealed and sturdy envelope that conceals its contents, or a tamper-evident envelope designed to reveal any interference with the contents. Ensure that the return address is for a locked mailbox and has the sender's name on it. Send the package through the United States Postal Service using first-class mail.

ii. **Hand Carried.** Store the Protected Information in a locked container or case or in a tamper-evident envelope.

iii. **Faxes.** The use of the University's Fax over IP services (XMedius) is authorized for transportation of HIPAA data, please see detail on pg., 39. When you transmit Protected Information by Fax:

(1) Use a cover sheet with a confidentiality notice requesting that faxes sent to an incorrect destination be destroyed and the sender notified. You may obtain a copy of a Fax Cover Sheet with this language on the Research Compliance pages on the Cutler Exchange.

(2) Confirm the fax number by voice call before the first use. Whenever possible, use tested, pre-programmed fax numbers.

(3) Confirm by voice call that the intended recipient is prepared to accept and retrieve the fax and, after transmission, that the fax was received.

(4) If you have job responsibilities that require the frequent faxing of Protected Information, make sure you have account access to XMedius software for this purpose. A request can be sent to CutlerTech@maine.edu.

(5) All instances of misdirected faxes involving Protected Information are treated as an adverse event and must be reported consistent with the Event Reporting Protocol.

iv. **Destruction.** When authorized or requested by the Principal Investigator responsible for the Protected Information, make sure to coordinate the destruction with the Technology Manager.

v. **Paper File Storage.** Store protected information documents in locked storage when they are no longer needed and awaiting destruction. The file box should clearly identify name of the Principal Investigator, project name and number, and the date when destruction of the documents is authorized.

6) How Do I Securely Handle Verbal Communication That Involves Protected Information?

Protected Information is sometimes transmitted verbally. For example, you may need to discuss conversations from a focus group with a colleague, or you may need to recruit focus group participants by phone call. When you must transmit Protected Information verbally, make sure you are not allowing unauthorized access by:

a) **Avoiding Conversations Where They Can Be Overheard.** When necessary, keep voices low and pay attention to unauthorized listeners to avoid unnecessary disclosures. When the employee's location or hardware is a hindrance to securing protected information that can be overhead, then the employee should discuss the issue with their supervisor and the project's Principal Investigator. Ideally, dictation and telephone conversations should be conducted where others cannot hear.

b) Protected Information should not be included in voicemail messages.

c) **Careful Use of Audio or Visual Records**. Avoid listening to or viewing video and audio recordings of Protected Information where unauthorized persons may be able to overhear or observe. The use of an encrypted audio recorder is required when recording Protected Information. The use of an encrypted audio recorder is recommended when recording Sensitive Information.

7) How Do I Keep My Workstation and Workspace Secure?

a) **Computers and Workstations.** An on-campus review of workstation security is completed by Cutler IT annually. Employees must also take the following measures to prevent unauthorized access to Protected Information through their computers and workstations:

i. **Use.** Employees are required to position their computer screens so Protected Information on the computer screen is only visible to those authorized to see it. Security monitor filters will be provided if screens are easily visible from a cubicle or office with the door open upon annual consultation with Cutler IT. Employees who work off-campus will need to ensure protected information is not accessible for viewing by unauthorized users by working in a private room, use of a privacy screen, or other means to ensure compliance. Employees are required to follow the Employee Protection of Data (APL VI-C), Acceptable Use of Information and Information Systems (APL- VI-H), and Remote work agreement and guidelines. University IT Information Security office provides Information security standards and policy.

ii. **Passwords.** Employees are required to use a strong password consistent with UMS and USM requirements. Passwords are required to be changed every six months in accordance with UMS policy. The password may not be shared with others, including other employees. If a password is learned by someone other than the authorized user, the employee must change the password immediately. For employees who routinely access Protected Information as part of their position, LastPass enterprise password management software with two-factor authentication will be provided upon annual consultation with CutlerTech.

iii. **Computers.** Cutler IT and UMS IT ensure the following:

(1) Workstation computer login security is handled by UAD Windows authentication.

(2) To decrease the frequency of false positive account locks, the UAD account will automatically lock after 10 failed login attempts within 5 minutes. Through the Password lockout policy (enforced by GPO), the enterprise computer will lock for 5 minutes before another login attempt can be made.

(3) All university enterprise machines have Microsoft Endpoint protection installed.

(4) Computer workstations with the university image will have the monitor screen automatically lock after 30 minutes of non-use.

(5) All University enterprise computers are required to have labeled property tags on each device.

(6) Computers that access PHI are required to do so through VPN with Multi-factor authentication and be part of an "SCCM" compliant computer collection that:

- Automatically install Falcon Crowdstrike software for additional endpoint protection and response.
- Automatically sets the monitor screen lock at 10 minutes of non-use.

iv. **Unattended Computers.** Employees are required to prevent access to unattended computers on and off campus according to the following guidelines:

(1) Employees must lock their workstations when they are left unattended during the workday either by logging off or locking the windows machine (Windows icon +L on keyboard).

(2) Employees must shut down their computers when leaving for the day.

(3) Anyone with access to PHI that does not work in a locked office must have a laptop cable lock installed and must use it prior to leaving for their space for the day. For off-campus use, employees must appropriately safeguard their university computing equipment as defined within the UMS Remote Work Guidelines.

(4) Employees must lock their campus offices when the employee leaves for the day or will be absent for an extended period. For those in cubicle areas, the spaces will be locked by the University between 5:30-6:00pm daily, Monday-Friday. Saturday and Sunday building access is only available by USM card.

v. **Storage.** Protected Information (including PHI) should not be stored on personal or university-assigned computer equipment. The University of Maine System provides restricted data file storage by UAD active directory groups for flat-file storage folders. IT System administrative provides SQL servers to the Cutler Institute and Advanced Computing Group. Restricted data servers (file and SQL) within the locked Data Center at Orono meet HIPAA and HITECH requirements with documented configurations, VEEAM backups, and Splunk reporting.

vi. **Remote Access.** Employees must use a university-owned encrypted laptop or if working as a contractor for the State, may use a State-owned encrypted laptop, when accessing Protected Information and comply with the Telecommuting Agreement consistent with the requirements of UMS Administrative Practice Letter VI-C and UMS Remote Work Guidelines.

vii. Malicious **Software Protections.** Employees:

(1) May not disable anti-virus software;

(2) Windows updates are pushed out monthly to all university enterprise machines via SCCM after careful testing by University IT. Software Center apps are updated and pushed out to devices as needed. If you work from home, you are required to connect regularly to the Viscosity UMS VPN profile, to receive Windows Updates monthly for the latest system and security updates.

(3) Immediately report virus infections CutlerTech;

(4) Do not open unexpected email attachments;

(5) Do not download documents from unexpected or unknown parties; and

(6) Do not download or install unknown programs from the web without CutlerTech approval.

(7) Do not provide credentials to unknown sources requesting them in a different way than you are accustomed to**. University IT will never request your login credentials electronically.** Please forward emails of this type to Phish@maine.edu

b) **Administrative Rights.** With limited exceptions, employees working with protected information will not have administrative rights on their Cutler-issued laptops. Employees may request consideration of an exception to this requirement for good cause by contacting Cutler's Technology Manager at CutlerTech@maine.edu. All requests are reviewed and approved by Cutler IT or escalated to Cutler IMT for further review.

8) What Do I Do When Things Go Wrong?

a) What Could Go Wrong? An adverse event is an incident that potentially results in unauthorized acquisition, unauthorized access, unauthorized disclosure, or other similar act that refers to situations where individuals other than authorized users have access or potential access to Protected Information; this includes situations where an authorized user acquires, accesses or discloses protected Information for a non-permitted use. **There are specific requirements, detailed below if the adverse event potentially affects 500 or more individuals.**

An adverse event might be the result of the actions of a university employee or someone outside the University. Types of adverse events include:

i. Unauthorized acquisition, access, use, or disclosure of protected information in a manner not permitted under the privacy rule which compromises the security or privacy of the protected information;

ii. A successful or unsuccessful attempt to disrupt system operations or breach system security, including network attacks or unwanted disruption, and viruses, worms, or other malware;

iii. The theft or loss of equipment, a physical intrusion or break-in, or social engineering (e.g. phishing); and

iv. A policy violation (*e.g*., the unauthorized use of someone's user credentials).

b) **What Do I Do Now?** No matter what your job is, you need to know what to do when things go wrong. See Administrative Practice Letter VI-C for a description of the responsibilities of all University employees. It is also important that you understand any obligations you have pursuant to a contract, other agreement or protocol governing the use of Protected Information specific to your project. As an example, a contract governing a specific project may include reporting timeframes that are more stringent than those required by Cutler polices. If you are unclear about what is required and/or how other requirements interface with our internal policies, please talk to the Compliance Coordinator.

c) **Reporting – Internal & External**. Within the Cutler Institute, you are responsible for:

(1) As soon as you become aware of a **potential or actual** adverse event, notify the individual designated as the Principal Investigator on the project. If the Principal Investigator is not available, notify the Project Director or the Compliance Coordinator.

(2) The Principal Investigator must complete the **Adverse Event web form** located on the Cutler Exchange as soon as you become aware. Once the form is submitted, it will automatically be forwarded to ORIO, the Cutler Compliance Coordinator, the Technology Manager, and UMS Information Security for their review and appropriate response or action. The PI should confirm that the webform has been submitted with the initial event reporter.

(3) The web form requires the following information:

- The nature of the Protected Information;

- The project funder; the source of the Protected Information, the law, contracts, subcontracts, and research protocols governing the Protected Information;

- When the Protected Information is about individuals, the number of individuals potentially affected by the Incident;

- What is known about who accessed the Protected Information, including names, the number of records if relevant;
- A description of the circumstances related to the adverse event.
- Any steps taken to contain the damage; and
- Any communications with internal and external parties.

(4) **The Office of Research Integrity and Outreach (ORIO) will initiate the investigation of the adverse event if it is related to a research protocol under IRB review and approval.** ORIO will interview the appropriate people to gather data about the incident. Upon review of the unexpected and related/possibly related event, the IRB will make the final determination as to whether the event constitutes an Adverse Event. Apart from institutional reporting obligations, it is the PIs responsibility to make reports of Adverse Events and unanticipated problems to the Sponsor and/or FDA, where required.

(5) If you have questions about completing the Adverse Event web form, the Compliance Coordinator or Technology Manager can provide assistance.

(6) Any adverse event involving ***Protected Health Information potentially affecting 500 or more individuals***:

- The Compliance Coordinator or Technology Manager shall notify the Program and Institute Directors.
- The Principal Investigator shall not inform any outside entities of any potential adverse event unless directed to do so by the Compliance Coordinator, ORIO, or Institute Director.

(7) The Principal Investigator, after reviewing contractual and regulatory requirements, is responsible for ensuring that all reporting requirements have been met after direction has been given to inform external entities.

(8) As appropriate, a referral of an employee's or student's violation of this policy to the employee's supervisor or University's Conduct Officer for appropriate action.

d) **Containment Basics**: In addition to completing the adverse event webform, if the adverse event involves paper, email, and malware, the following steps should be considered.

(1) **Paper:** Seal a paper document or an unencrypted electronic device in an envelope and write the date and time across the seal. Store the envelope in

a locked filing cabinet.

(2) **Email**: Delete an email you received from your inbox and your trash file immediately. Notify the sender immediately. If you sent the email, call the recipient of the email, and ask them to destroy the email from both their inbox and trash folders before it is opened. Delete it from your sent folder.

(3) **Malware or Virus:** Notify the Cutler Technology team immediately.

(4) **Other containment** steps may be recommended based on the review of the adverse event webform details by the Adverse Event response team (ORIO, Information Security, and designated Cutler resources).

d) **Whistleblower Protection:** In accordance with UMS APL IV-J, retaliation against anyone who, in good faith, reports a violation of these policies is prohibited.

e) **Any Other Noncompliance Concerns.** Staff may anonymously report a concern or issue related to any compliance issue, including but not limited to specific events, practices, and procedures. Staff may complete the Non-compliance Event web form.

f) **Help Us Learn from Our Mistakes**: Whenever a problem occurs as the result of a preventable error, we want to learn from that mistake and must always evaluate what we can do to prevent an error from occurring in the future. Even when someone outside the university commits an error, we should evaluate whether there is something we can do to prevent the same mistake from happening again.

C. For Principal Investigators

1) Why Me?

Within the Catherine Cutler Institute, responsibility for managing our project work is decentralized to Principal Investigators. As the Principal Investigator, you have accepted responsibility for conducting your project in accordance with university policy, any contract that governs your project, and any federal or state law that governs your project. When it comes to Protected Information, it makes sense for you to take responsibility because you are in the best position to:

a) Know whether your project involves Protected Information.

b) Design your project and develop your project work plan and budget to ensure that you have the time and resources you need to comply with any legal requirements.

c) Ensure project staff understand their role in your project as it relates to Protected Information.

d) Ensure project staff understand how the Protected Information for your project may be used or disclosed and how it must be secured.

e) Ensure that any potential or actual adverse event connected to your project is reported and handled in a manner most likely to mitigate harm to the individuals whose Protected Information is potentially breached, to the university, and to external client relationships. This policy and other resources available on the Cutler Exchange are intended to help you do your job.

2) What Do I Need to Do When I Design a Project?

When you are designing a project, you need to:

a) **Know What Protected Information You Need.** You need to know when your project involves Protected Information and design it to use only the Minimum Necessary to accomplish your project goals. See Section 3 below.

b) **Develop a Data Management Plan.** If you need Protected Information to complete your project goals, develop a Data Management Plan that:

i. Describes the purpose of your project.

ii. Identifies the Minimum Necessary Protected Information to achieve your project goals.

iii. Identifies the level of access to the Protected Information that will be needed by different staff members or roles. For example, those conducting a survey may need access to Direct Identifiers. In contrast, those responsible for analyzing the survey results may only need access to Indirect Identifiers (*e.g.*, zip code), or they can do their analysis using De-Identified Information.

iv. Identifies the individual responsible (e.g., Data Custodian) for the physical possession or storage of the Protected Information.

v. Identifies the plans for the physical storage and possession of the Protected Information (*e.g.*, the compliant server or the encrypted device on which it will be temporarily stored). Identify who will manage the raw data for the team, what is the raw data storage size needed, and what data file type(s) will be sent from the data provider.

vi. Identifies any uses or disclosures of the Protected Information needed to accomplish project objectives.

vii. Identifies how long you expect the data will be retained after the project ends and your plans for destroying the compliant data, as required by the IRB, contract or law.

c) **Allow For Extra Time.** Factor in additional time for gaining access and approval to acquire, create, use, or disclose the Protected Information. When you are budgeting time:

i. At a minimum, you need to factor in any additional time needed to get an agreement allowing you to use the Protected Information signed by both parties;

ii. Especially if this is a new relationship or partner, you may also need to add additional time to allow for negotiating the terms of the agreement. If you have already been through this process with the same party for the same kind of agreement, it is likely to take less time than the first time. However, if it's a new partner, hope for the best but plan for the worst: legal review may slow the process down considerably.

iii. Any due diligence you may need to do to be confident that a subcontractor can handle and secure the Protected Information. See Section 5 for more information. If IRB approval is needed, plan to submit 30 days before acquiring data.

iv. If a Business Associate Agreement or Data Use Agreement is needed, allow for extra time for that approval process.

v. No Protected information will be accepted from an external entity without an executed agreement between Cutler and the external entity and/or between the external entity and the USM IRB (if applicable). Therefore, sufficient time should be allowed to negotiate and obtain the required executed agreements.

d) **Allow for Extra Costs.** Factor in any additional expenses related to the Protected Information, including the costs of:

i. Purchasing the Protected Information, if applicable;

ii. Any additional staff time associated with acquiring the Protected Information, training staff, managing its use, or other activities related to Protected Information;

iii. Securing or transmitting the Protected Information, including storage/server fees or the purchase of encrypted devices;

iv. Assuring that a subcontractor can provide the required level of security. (See Section 5);

v. Compensating a subcontractor for any additional costs associated with securing, transmitting, or handling the Protected Information.

3) How Do I Get Access to Protected Information?

Depending on the kinds of protections that apply to your Protected Information, there are several steps to take before you can access or create Protected Information for a project:

a) **Categories of Protected Information.** Typically, how you get access to Protected Information depends on the kinds of protections that apply to it. Below are some of the types of protections typically encountered in our work.

i. **Information under the Protection of a Responsible Party.** A Responsible Party is any entity given responsibility for the protection of certain types of information under state or federal law. For example, under HIPAA, a Covered Entity is a Responsible Party for Protected Health Information. Under FERPA, the university is a Responsible Party for educational records. Typically, a law will define:

(1) The information that is protected;

(2) The purposes for which it may be used; and

(3) To whom it may be disclosed and under which conditions.

Any time you want to acquire, use, collect, create, or disclose information under the protection of a Responsible Party, you need to make sure you have the Responsible Party's permission to do so. It is up to the Responsible Party to make sure that permission is granted only as allowed under the law.

To get access to information under the protection of a Responsible Party, we enter a contract with the Responsible Party. The contract should define what information we may use, for which purposes, to whom it may be disclosed under what conditions, and how/when it should be eventually destroyed. The contract will also define the requirements for making sure the Protected Information is handled and stored securely.

ii. **Information Protected under a Research Protocol. If you are conducting a research protocol that requires the disclosure of Protected Information, you will need the required Agreements between Cutler and the entity you are obtaining the information from. The USM IRB will review the Agreement prior to approving or disapproving a protocol.** In this case, the Principal Investigator is the party responsible for ensuring the Protected Information is used or disclosed only as allowed under the research protocol.

iii. **Business Associate Agreements (BAA). If your project requires a BAA, you will need to review the Standard Operating Procedure (SOP) memo issued by ORIO outlining the review, approval, and training requirements for BAAs ("USM as Business Associate Component").** A Business Associate (BA**)** is a person or entity who, on behalf of a covered entity, performs or assists in the performance of a function or activity involving the use or disclosure of individually identifiable health information, such as data analysis, claims processing or administration, utilization review, and quality assurance reviews, or any other function or activity regulated by HIPAA. A covered entity is defined to be 1) health plans, (2) health care clearinghouses, and (3) health care providers who electronically transmit any health information in connection with transactions for which HHS has adopted standards. A subcontractor(s) who creates, receives, maintains, or transmits Protected Health Information on behalf of a BAA is a -Business Associate under HIPAA Regulations. The Office of Research Integrity and Outreach (ORIO) serves as a repository for all executed BAAs. The SOP can also be accessed online at: https://usm.maine.edu/orio/wp-content/uploads/sites/361/2022/08/HRPP-016-USM-as-Business-Associate-Component.pdf

b) **Before You Acquire or Create Protected Information Make Sure You Are Authorized or Permitted to Do So.** Depending on the type of Protected Information, whether you will be acquiring it from a Responsible Party, collecting or creating it on behalf of a Responsible Party, or acquiring, collecting, or creating it for research purposes, you have one or more steps to complete before you may begin to access or create the Protected Information:

i. **Make Sure You Have All Required Signed Contracts and Research Protocol approvals documents in Place.**

(1) **Contracts with the Responsible Party**. The Responsible Party is responsible for ensuring a contract is in place that defines the Protected Information and its Permitted Uses and Disclosures. However, when you are aware of the potential need for a contract, as a professional courtesy, you should raise the question if the Responsible Party's agent fails to do so.

(2) **Subcontracts on Behalf of a Third Party**. If you are contracting with a third party to collect or create the Protected Information on behalf of a Responsible Party, it is your responsibility to make sure the subcontract with the third party complies with your contract with the Responsible Party. For example, if you are conducting a survey on behalf of a Responsible Party (*e.g.*, a state agency or provider agency), refer to your contract with the Responsible Party to make sure you have the authority to enter the subcontract. Then make sure your subcontract is consistent with the terms of your agreement with your Responsible Party.

(3) **Other Contracts**. If you contract with a third party to collect, use, store, or otherwise handle Protected Information on your behalf, you still must confirm that you have authority to do so. For example, if you are conducting a survey as part of a research project, refer to your IRB-approved research protocol to make sure you have the authority to contract with the third party in this way and to make sure your contract with the third party is consistent with the terms of your research protocol.

(4) **IRB-Approved Research Protocol.** You will need IRB approval to acquire or create Protected Information any time you are conducting Human Subject Research. If you have any questions as to whether you are conducting Human Subject Research, submit a Request for Determination of Research Involving Human Subjects to the IRB. ONLY the IRB can determine if you are conducting Human Subject research. Consult with the Office of Research Integrity and Outreach if you have any questions about whether you are conducting research.

ii. **Make Sure Your Contract, Subcontract or Research Protocol Defines Protected Information, Permitted Uses and Disclosures, and Data Destruction Information**: Your goal is to make sure your contract or research protocol define the Protected Information you will need, and how you will use or disclose it, as necessary to accomplish your project goals or conduct your research. That means you need to:

(1) **Clearly state your project objectives.** If you want to have permission to use or disclose the Protected Information as necessary to accomplish your project objectives, be sure your project goals are clearly stated. For example, your project objectives might say that you and your project staff will review case records as necessary to assess a provider's fidelity to a particular model of care. Your project objectives must be consistent with what is permitted under the law. For example, if eligibility data can only be used for the proper administration of the TANF program, then your project objectives must be consistent with the goal of supporting the proper administration of the TANF program.

- **For subcontracts:** You may not grant a subcontractor greater authority than you have been granted. That is, you must ensure that the subcontractor's permitted use and disclosure align with what your contract (or IRB protocol, if applicable) says you may permit under the subcontract.

(2) **Define the Minimum Necessary Information required to achieve project objectives.** Your goal is to be unambiguous but not so specific that you have to amend your contract or research protocol with every minor change in your method. For example, unless you are required to by a Responsible Party or the IRB, or you have absolute certainty, do not itemize the specific data elements as the Minimum Necessary. Instead, use broad categories (*e.g*., Medicaid claims with Direct Identifiers omitted but including Indirect Identifiers).

(3) **Describe Permitted Uses and Disclosures.** Make sure your contract or protocol is unambiguous about the purpose for which Protected Information may be used (*e.g.*, as necessary to accomplish project objectives, with your project objectives clearly identified). If you anticipate needing to disclose the Protected Information, make sure you identify what Protected Information may be disclosed, to whom, and for what purpose. If you are uncertain about to whom you will disclose the Protected Information, you can specify the criteria for selecting that third party (*e.g.*, the third party has met widely recognized auditing standards) or the process for selecting the third party (*e.g.*, as mutually agreed to by the Responsible Party).

(4) **Describes Data Destruction information.** Data destruction information should include any required data destruction methods or guidelines, timelines, and destruction communication requirements (i.e., letter or certificate of destruction).

iii. **Make Sure Your Authority or Permission is In Effect.** As applicable, you do not have authority or permission unless:

(1) Your contract is signed by the responsible party, by the university's authorized signatory, and the contract has not expired.

(2) Your research protocol is approved by the IRB and has not expired.

iv. **Amend Your Contract or Research Protocol When You Need Different Permissions.** The Principal Investigator is responsible for ensuring that a contract or research protocol is amended when there is a need to change:

(1) The definition of the Protected Information or Minimum Necessary;

(2) The purpose for which it may be used; or

(3) The conditions for disclosing the Protected Information to a third party.

v. **Complete the Compliance Resource Request Form for your new project**. As part of this request and **before** compliant space is allocated for your project, you will need to provide evidence that the covered entity or data provider has given permission to store the data. This may include one or more of the following:
(1) A contractual agreement that confirms funding for the research project or service.
(2) A BAA or Data use agreement that confirms we are authorized to use the protected data.
(3) An IRB or Privacy Board approval letter or waiver of individual authorization, if applicable, which confirms the research and methods have been authorized. If the IRB determines the work is not research, then documentation is not required but will be noted in PIMS.
(4) A data request form or a letter of support from a state entity such as MHDO indicating they support access to the data of the proposed project.

vi. Once submitted, the Technology Manager will review and follow up with you to gather final details, update PIMS, create or coordinate the compliant resources and access requested, and communicate with the PI when the resources are available and PIMS is ready for review.

vii. **Make Sure the Protected Information is Transmitted Securely.** See Part B, Section 4 above for more information about transmitting Protected Information securely.

4) What Do I Have to Do When I Get the Protected Information?

If you have written your Data Management Plan well, you have a roadmap for what to do once you acquire, collect, or create Protected Information. Below is a list of several basic steps:

I. **Store the Protected Information securely.** See Part B, Section 4 for more information about secure storage.

II. **Ensure the Protected Information in the Cutler Protected Information Management System (PIMS) is accurate**. PIMS is a database created to track electronic Protected Information associated with individual projects. (That is, you do not need to use PIMS for individually identifiable information handled solely for the internal administrative purposes of the university, *e.g*., individual identifiers used for reimbursement).

III. **Data Sets**. A Data Set is the unit of Protected Information tracked in PIMS. A Data Set is a logically meaningful grouping or collection of information that includes Protected Information. A Data Set may be electronic Protected Information or Protected Information stored in any other format. A Principal Investigator should ensure:

a) Data Sets only include Protected Information;

b) For each set of Protected Information that includes *different data or formats,* each set is recorded separately;

c) The right Data Sets are connected to the correct projects; (PIMS is organized by project number, so Data Sets should only be related to work performed under that project.)

d) Two sets of the same Protected Information stored in different formats but with the ***same authorized users***, are recorded ***as separate data sets***;

e) Two sets of the same Protected Information but ***with different authorized users***, should be recorded each as ***two separate Data Sets***; and

f) Storage location, a brief description of the data, the scheduled destruction date and method (see Section 4.d), authorized users, formats and any extracts made.

ii. **Delegation**. The Principal Investigator may delegate responsibility for reviewing Protected Information in PIMS to a Project Director. However, the Principal Investigator retains responsibility to ensure all data sets are listed in PIMS.

IV. **Create Copies and Extracts Only as Permitted.** The Principal Investigator ensures that copies and extracts of Protected Information are only created as permitted under the legal terms governing the Protected Information. If a copy or extract includes Direct or Indirect Identifiers or otherwise is still Protected Information, responsibility for the copy or extract is assigned as follows:

i. If the copy or extract was created for use under the Principal Investigator's Project, the Principal Investigator is responsible for safeguarding it in compliance with all aspects of this policy;

ii. If the copy or extract was created for use under another project, the Principal Investigator receiving the copy or extract is responsible for safeguarding it in compliance with all aspects of this policy; or

iii. If the copy or extract was created for use by a third-party external to the Muskie School, the Principal Investigator maintains responsibility for the Protected Information and may disclose the copy or extract only as permitted under the legal terms governing the Protected Information and, if required, subject to a subcontract in compliance with Section 5.

V. **Train Project Team.** The Principal Investigator trains project staff on

i. What uses and disclosures are permitted;
ii. Where the Protected Information may be stored;
iii. Members' responsibilities and the Minimum Necessary information to which team members have access;
iv. Approved methods for safeguarding the Protected Information, and
v. Other details necessary to comply with the terms of any applicable contract, IRB protocol, or any other terms governing the Protected Information.

VI. **Monitoring and Directing Staff.** The Principal Investigator monitors project staff's compliance with the legal requirements governing the Protected Information and the security practices defined under this policy. The Principal Investigator reports violations to the employee's supervisor and ORIO (if applicable), consistent with Section 8.

VII. **Terminating Access.** The Principal Investigator is responsible for terminating access to Protected Information if a member of the project staff no longer needs to access the Protected Information. Upon removal of access to project-related PHI, the Principal Investigator is also responsible for retrieving all original documents or copies and extracts containing Protected Information in the staff member's possession.

VIII. **Violations.** When a member of the project staff is found in violation of the legal terms governing the Protected Information, university policy, or this policy, the Principal Investigator has the following responsibilities and authorities:

i. **Reports to Supervisor.** The Principal Investigator reports a violation to the individual's supervisor or the University's Conduct Officer for student violations;

ii. **Reports to the IRB**. The Principal Investigator shall report a violation to the IRB if the protocol is an IRB-approved research project.

iii. **Terminates Access.** The Principal Investigator may terminate the employee's or student's access to Protected Information associated with the Project;

iv. **Terminates Project Funding Allocation.** The Principal Investigator may terminate the allocation of Project funding to an employee's salary if, after notifying the employee's supervisor of the violation, termination of funding has been determined an appropriate disciplinary action following proper due process conducted with the guidance of the University's Human Resources and consistent with the applicable collective bargaining agreement.

5) What Do I Need to Know About Subcontracts and Protected Information?

Before you can contract or subcontract with a third party to handle or store Protected Information, you must confirm that you are authorized or permitted to do so. If you are contracting with a third party to handle Protected Information on your behalf, you are responsible for assuring that the third party has the capacity to safely handle and secure the Protected Information. You also have a responsibility to protect the university from any avoidable risk. The level of due diligence required will depend on the level of risk associated with the contract or subcontract. The level of risk will be higher if you are working with a large volume of individuals (e.g., 500 or more), PHI, or High-Risk Identifiers. Consult with the UMS Chief Information Security Officer to determine the appropriate level of due diligence.

a) **Contract or Subcontracts.** Your contract or subcontract with the third party should address a number of important elements:

   i. **Minimum Necessary and Permitted Uses and Disclosures.** What Protected Information the third party will have access to and the purpose for which it may be used, and the permitted uses and disclosures of the Protected Information by the subcontractor. The Principal Investigator ensures that the subcontract does not grant access to Protected Information except as authorized or permitted under the legal terms governing the Protected Information.

   ii. **Standard Template.** All subcontracts use standard subcontract templates approved by University's Office of General Counsel. Any modification to the standard subcontract terms is subject to the review and approval of the University's Office of General Counsel.

   iii. **Subcontract in Effect.** When required, the Principal Investigator ensures that a subcontract is in effect before Protected Information is disclosed to a third party or the Principal Investigator causes a third party to acquire or create Protected Information on behalf of the university. A subcontract is in effect when the authorized signatory for the university signs it. A subcontract is not required if the university, in its capacity as a Business Associate to a Covered Entity and as authorized or permitted under the legal terms governing the Protected Information, is disclosing Protected Information to another Business Associate of the same Covered Entity. If a BAA is required as part of the subcontract, you will need to review the standard operating procedure (SOP) memo issued by ORIO outlining the review, approval, and training requirements for BAAs[1].

   iv. **Amending Subcontracts.** When permitted by the legal terms governing the Protected Information, university policy, and this policy, the Principal Investigator is responsible for ensuring that a Data Use Contract is amended when there is a need to change:

      (1) The definition of the Protected Information to be provided or created;

      (2) The definition of who may access or use the Protected Information;

      (3) The conditions for disclosing the Protected Information to another party; or

[1] https://usm.maine.edu/orio/wp-content/uploads/sites/361/2022/08/HRPP-016-USM-as- Business-Associate-Component.pdf

(4) Any other significant provision of the subcontract.

v. **Corrective Action.** If you become aware of a pattern of activity by the third party that seems like it might be a significant breach or violation of the third party's responsibilities under its contract with the university, consult with the University's Office of General Counsel. The University General Counsel can help you evaluate the situation to determine whether you need to take any corrective action or terminate the agreement.

D. For Supervisors

1) What Should I Be Thinking About When I Hire a New Employee?

If you are a supervisor, you should consider a new employee's roles and responsibilities for Protected Information when developing a job description and selection criteria and planning for training, workstation, and other onboarding elements. The supervisor should make sure that:

a) The required qualifications for the new employee reflect the skills and knowledge needed to fulfill that employee's responsibilities for Protected Information;

b) The new employee's job description adequately describes the employees' roles and responsibilities relative to Protected Information;

c) The appropriate background screening is conducted by Human Resources;

d) A secure workspace is available for a new employee who will be handling high volumes of Protected Information;

e) A new employee signs a Confidentiality Agreement, if required for fulfilling his or her job functions. You must require a Data Custodian and any other employee whose job responsibilities involve handling Protected Information to sign this agreement. See *University of Maine System Template Employee Confidentiality Agreement*, accessed at Administrative Practice Letter VI-C, Appendix B.

f) A new employee who works at home or non-university locations or who uses non-university devices understands his or her responsibility for complying with the measures identified in the UMS *Administrative Practice Letter VI-C, Appendix A: Protection of Compliant Data*[2] when using non-university devices or networks.

g) A new employee receives all training (including HIPS CITI Training) necessary for fulfilling his or her job responsibilities, including the responsibilities of a Data Custodian or Principal Investigator.

2) What Are My Responsibilities for Ongoing Supervision?

A supervisor's responsibility for ensuring that employees are appropriately qualified,

[2] https://www.maine.edu/apls/apl-vi-c/

equipped and trained to handle Protected Information is ongoing. These responsibilities include making sure:

a) The employee stays current with all training required to perform his or her job responsibilities.

b) You and the employee update the employee's job description and job qualifications to reflect these changes.

c) The University's Human Resources Division initiates a performance improvement plan or sanctions, as appropriate, when an employee violates UMS, USM, or this policy, the applicable collective bargaining agreement, or the Confidentiality Agreement, that complies with the applicable collective bargaining agreement.

3) What Do I Need to Remember When an Employee Leaves the Cutler Institute?

As the supervisor, you will need to coordinate with Human Resources and review guidance for employee departures. (See Section E, Resources.) You must:

a) Oversee and coordinate with CutlerTech the return of all technology hardware and devices and the surrender of any Protected Information held by the employee. Requests can be made to CutlerTech@maine.edu.

b) Inventory any Protected Information for which the employee is responsible. CutlerTech can provide a report from PIMS to assist PIs with employee departure plans. Requests can be made to CutlerTech@maine.edu. The Cutler Technology Manager will provide support and update PIMS project information as required.

c) Ensure that access rights are terminated or changed.

   i. In the case of a voluntary termination, make sure that CutlerHR@maine.edu and CutlerTech@maine.edu are notified at least a week in advance of termination;

   ii. In the case of an involuntary termination, notify CutlerHR@maine.edu and CutlerTech@maine.edu **before** notifying the employee. Collect all devices in which PI or PHI may have been stored at the time of departure.

   iii. Ensure that research PI responsibilities are transferred to a new PI, as appropriate. Contact the PIMS administrator/Cutler Technology Manager at CutlerTech@maine.edu for a list of their projects.

d) Principal Investigators who are departing are responsible for ensuring that human subject research-related duties are transitioning in accordance with policies and procedures of the Office of Research and Integrity and Outreach, specifically HRPP-005. (See Section E, Resources.)

E. Resources

1) Contacts

Cutler Institute Resources		
Lindsey Smith, Compliance Coordinator	m.lindsey.smith@maine.edu	228-8370
Sara Abronze, Technology Manager	sara.abronze@maine.edu	780-5774
Cutler Technology Team	cutlertech@maine.edu	
Information Security Office	infosecurity@maine.edu	581-3590
Office of Research Integrity & Outreach	usmorio@maine.edu https://usm.maine.edu/orio	780-4517
IRB	https://usm.maine.edu/orio/collaborative-institutional-review-board-irb/	

2) The Technology/Compliance page on the Cutler Exchange.

This webpage includes additional information and resources: https://cutlerexchange.net/technology-comunications/.

3) Web Forms

Located on Cutler Exchange: https://cutlerexchange.net/forms/

a) Adverse Event

b) Noncompliance Concern

c) Compliant Resource Request form

d) SFTP Secure Transfer Request

4) Access to Cutler Information Systems and Protected Information Procedure

a) A background check is completed on all new hires. Once this is complete, an employee identification number is generated.

b) Through the Cutler Technology Access Request web form, the employee's supervisor requests access to the university network and identifies the specific network locations this employee will need to access.

c) The employee receives a picture ID, and the supervisor must complete a card access request form for the locations, such as their office or workplace, they need access to at USM in either Portland or Augusta as appropriate.

d) Once a UMS account has been created and activated for the new hire, access can be given to employees whose job requires them to review protected information via the Protected Information Management System (PIMS) by following these steps:

i. The Project Director requests a protected information resource (i.e. compliant storage folder SQL space, encrypted device, paper, etc.) from the Technology Manager by completing the Compliant Resource Request web form located on the Cutler Exchange.

ii. The Principal Investigator and/or Project Director should identify the data source and access requirements for each project staff member within the Compliant Resource Request Form. The Principal Investigator and/or Project Director provide the information to the Technology Manager, who will input the information as described into the Protected Information Management System (PIMS) and assign each staff member the appropriate access to the data resource and virtual private network (VPN) with two-factor authentication. In addition, the Technology Manager will also supply or coordinate the network access as described.

iii. PIMS tracks protected information, including the date the file is created, user access, type of authority for the use of the data (e.g., DUA, BAA, IRB), and required method and date of compliant data destruction.

iv. The Principal Investigator (PI) or Project Director (PD) is responsible for determining when to terminate access and notifies the Technology Manager. In addition, access will be removed by the Technology Manager when a team member’s employment has ended. When this occurs, a notification will be supplied to the Principal Investigator (PI) and Project Director (PD), as listed in PIMS, that the staff member’s access has been removed and any required communication with the grant funder should occur.

v. The Principal Investigator (PI) or Project Director (PD) and Technology Manager are responsible for reviewing all information in PIMS and keeping it updated and current. The Technology Manager will assist PIs/PDs with data entry into PIMS.

vi. The Technology Manager is responsible for monitoring PIMS Data destruction dates and will alert the Principal Investigator, Project Director, and Grants & Contract Manager when an upcoming data destruction date for the project has passed. The goal in monitoring is to confirm continued authorization and flag any issues with ORIO and the Research Service Center when authorization is not provided.

e) When an employee departs the Cutler Institute all compliant data network and server access listed in PIMS for the employee is removed the first business day after an employee departs by the Technology Manager. In addition, the computer is either wiped or imaged, removing all user data or files stored on the hard drive.

f) When terminates employment at the university, a Supervisor Departure Form is completed on-line. Human Resources notifies University IT, who then terminates the employee's access based on the UMS User Account Management Lifecycle and IT supported Systems Off-Boarding.

g) If the university terminates a position, access removal is coordinated with IT staffon the day of termination.

5) Protected Information Management System (PIMS)

https://apps.maine.edu/MuskieProtectedInfo/

The Protected Information Management System (PIMS} was designed for Cutler Institute administration, Principal Investigators, and Project Directors to manage, track, and destroy protected information as required by research-related project IRB or contractual agreements.

Therefore, PIMS's:

- Tracks compliant resources on a given project regardless of location or format
- Identifies who has access to each of compliant resources
- Tracks data destruction dates and planned destruction methods
- Track extracts you make for use by other Cutler Institute staff or external parties

a) Who Uses PIMS and Why

The **Principal Investigator** is the person identified by the Research Service Center as the single point of accountability for an externally funded project. This web portal will display each Principal Investigator's active projects with restricted data from the University of Southern Maine's PeopleSoft/GL Inquiry system. However, Principal Investigators can request PIMS project access for their **Project Directors**. It is the expectation that PIs/PDs know how to navigate PIMS to review their project's restricted data, access, and upcoming data destruction. PIs and PDs should work directly with the Cutler Technology Manager when any changes are necessary on their PIMS's projects.

The **Technology Manager** enters compliant details for each project and ensures the data sets are created specifically for the resource type, destruction method, and user access. In addition, provides & updates staff access and reports to the Cutler Integrated Management Team, ORIO, and University IT on utilization or compliance concerns. Lastly, reports to the Principal Investigator, when data sets on a project are overdue for data destruction and require next steps or further discussion.

b) Training

An annual training refresher will be provided by the Cutler Technology team each year. New PIs/PDs should request on-demand training, as part of their onboarding, with the Cutler Technology Manager.

6) Requirements for Departing Principal Investigators

https://usm.maine.edu/orio/wp-content/uploads/sites/361/2022/08/HRPP-005-Departing- Principal-Investigators.pdf

7) Guidance for Employee Departure

https://sites.google.com/maine.edu/usmemployeeresources/departing-employees

8) ORIO SOP HIPAA-001 USM as Business Associate Component

https://usm.maine.edu/orio/wp-content/uploads/sites/361/2022/08/HRPP-016-USM-as- Business-Associate-Component.pdf

9) Secure Fax over IP (FoIP)

The use of the university's Fax over IP services (XMedius) is authorized for transportation of HIPAA data as long as the following guidelines are adhered to.

- Until such time that networked Multi-Function Printers (MFP) are configured to use encryption to communicate with the XMedius server they cannot be used for faxing, printing, or scanning HIPAA/ePHI documents.
- Until such time that networked scanners are configured to use encryption to communicate with the user’s computer or XMedius server they cannot be used for scanning HIPAA/ePHI documents.
- Until such time that networked printers are configured to use encryption to communicate with the user’s computer or the XMedius server they cannot be used for printing HIPAA/ePHI documents.

The university email system is not approved to store ePHI. The following restrictions are also in place when working with ePHI/HIPAA documents.

- Faxed documents received by the university containing ePHI may not be sent via email, whether directly from the Xmedius server or from a MFP.
- Faxed documents sent by the University containing ePHI may not be sent via email to the XMedius server or a MFP.

Use of fax services through the XMedius server is only authorized for HIPAA/ePHI in the below configuration.

Outgoing Fax over IP

Faxes containing HIPAA/ePHI data must originate from the Xmedius server. This can be accomplished by using the Xmedius web application. Paper documents containing HIPAA/ePHI data may be scanned to the user's computer for faxing using a standalone scanner or MFP connected directly to the computer (i.e., through USB, SCSI, Firewire, parallel port, or similar non-networked connection). The document may then be transferred to the XMedius server through the web application.

Incoming Fax over IP
Faxes containing HIPAA/ePHI data must only be accessed through the XMedius web application and must not be automatically forwarded to a university email account.

If a project would like a fax number specifically for transmitting restricted data via fax over IP (FoIP) with the Xmedius server, please email your request to CutlerTech@maine.edu

10) Secure Printing

Secure printing can be conducted on UMS: IT-deployed Xerox multi-function printers. Using this method, print jobs are securely transmitted to a secure PaperCut print server and then printed only when the user's campus card is presented at a Xerox printer. The print content is not stored on the printer.

A printer connected directly to the computer (i.e., through USB, SCSI, Firewire, parallel port, or similar non-networked connection) is also permitted.

11) Maine Care - OMS Claims Data- Technical Press

https://umainesystem.sharepoint.com/:b:/s/USM-CutlerInstitute/EWdwKXd1WYpOs_MPDsQCyI8BBNzjeEEsmZa1rSob7XT2tw?e=djV8Yy

12) Survey Research Center Privacy Guidelines-

https://www.srcmaine.org/privacy-guidelines/

13) Survey Respondent FAQs-

https://www.srcmaine.org/survey-respondents-frequently-asked-questions