ULSTER COUNTY
HIPAA / HITECH COMPLIANCE PROCEDURES

Jen Metzger
County Executive

February 2019
(REVISED December 2020)
(REVISED November 2021)
(REVISED September 2022)
(REVISED January 2023)
(Revised December 2024)

TABLE OF CONTENTS

County Compliance Officer: Tom Gibney
tgbn@co.ulster.ny.us
(845) 340-8771

County Privacy Officer: Clint Johnson
cjoh@co.ulster.ny.us
(845) 340-3685

County Security Officer: Alan Macaluso
amac@co.ulster.ny.us
(845) 334-5564

County Compliance Hotline: The Bonadio Group
(877)569-8777

Procedure: *HIPAA/HITECH Compliance*
Topic: *Access Request Processing*

HIPAA Regulation:

- *Access* § 164.524

Purpose:

The purpose of this procedure is to provide individuals with the opportunity to access and obtain copies of their health information in accordance with the HIPAA requirements.

Description:

It is the procedure of the **County of Ulster** that access to protected health information (PHI) must be granted to the person who is the subject of such information when such access is requested, or at the very least within the timeframes required by the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule and any relevant State law.

It is the procedure of **County of Ulster** to inform the person requesting access of the location of PHI if the Organization does not physically possess such PHI but has knowledge of its location.

Responsibilities: Staff person

1. Forwards all requests for access or copying of PHI to Privacy Officer.

Department Privacy Officer/Designee

1. During the initial contact (or within 10 working days of the initial contact), informs the individual or his/her personal representative that requests must be submitted using the Request for Access to Protected Health Information Form.
2. Verifies identity of the individual or personal representative.
3. Provides the individual or his/her personal representative with a copy of the Request to Access form either in person or by mail or fax.
4. Provides assistance in completing the form, if requested.
5. Tracks the status of the request on the Request for Access Tracking Form.
6. Reviews the Request for Access to Protected Health Information Form as soon as it has been received to determine:
    a. The exact amount and nature of information requested.
    b. Where that information is kept.

c. Whether the requestor requires access copies of the information, a summary of the information, or some combination.
d. Whether the individual requests the copy to be sent directly to another person and has identified where the copies should be sent.
e. The format (paper, electronic) of the requested records.
f. The format (paper, electronic) of the requested copies, if any.

7. Performs initial review of request to determine if the information is available for review.
8. Directs the individual to the appropriate department, if the information requested is not kept by the department, but the location is known.
9. Reviews the access request within 10 working days of receipt of the request and determines if the request will be granted or denied.
10. Documents the granting or denial of access in the Response to Request for Access to Protected Health Information Form.
11. Informs the requestor of the determination. Sends a copy of the Response to Request to Access to the requestor by certified (receipt) mail.
12. If request is denied, and at the individual's request, refers denial information to Department head/Designee. **(See NOTE below)**

NOTE: According to federal regulations, requests for access may only be denied for the following reasons:

- The requested information is held by a clinical laboratory or other entity that is exempt from the Clinical Laboratory Improvement Amendments.
- The information is in the form of psychotherapy notes.
- The requested information was compiled in anticipation of or for use in a civil, criminal, or administrative proceeding.
- The protected health information was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.
- The information was disclosed to the provider on the condition that the information would never be disclosed to any other party. (If the Department has disclosed the information to any other person, the information must be included in the clinical record.)
- A licensed health care professional has determined, in the exercise of professional judgment, that the access may endanger the individual or someone else.
- The information refers to another person (other than a licensed health care provider) and the provider has determined in professional judgment that the other person may be substantially harmed.
- A personal representative made the request and a licensed health care provider has determined in the exercise of professional judgment that the provision of access is reasonably likely to cause substantial harm to the individual or someone else.
- An organization that is a correctional institution or is functioning on their behalf may deny access to inmates.

If Access Request is Granted:

Department Privacy Officer/Designee

1. Ensures that the response clearly states the fees incurred for copying (if any).
2. Within 10 working days of the determination to grant access, arranges for a convenient time for access. The access should be completed at the earliest time convenient to the requestor but within 30 days of the determination to grant access. (*According to the HIPAA Privacy Rule, the Organization can obtain an additional 30 day extension.*)
3. Arranges for any copying within 10 working days of notification to the requestor. ***(See NOTE below.)***
4. If applicable, calculates the total amount to charge for copying. Department should determine reasonable cost based fee for copies (paper or electronic media) or for preparing a summary of the requested information, if applicable. (If the Department determines the requestor is unable to pay the charge for processing the request, the Department will provide the requested access.)
5. Is present when the individual or his/her personal representative appears at the scheduled time and at all times when the requestor is reviewing any original records.
6. Files all completed Requests and Responses in the Department HIPAA compliance file. Does *not* file with the individual's clinical record.

NOTE: If an individual requests an electronic copy of information that is maintained in the clinical record, the Department must provide the individual with access to the information in the electronic form and format requested. However, if the information is not readily producible in the requested form and format, the Department must provide the information in a readable electronic form and format agreed to by the Department and the individual.

If Access Request is Denied:

Department Privacy Officer/Designee

1. Ensures that the requestor is granted access to all information that is not subject to the grounds for the denial.
2. Informs the requestor of findings. Sends a copy of the Response to Request Access to the requestor by certified (receipt) mail.
3. Informs the requestor of the right to obtain a further review of the denial by the Department Head/Designee.
4. If the requestor requests such a review, forwards all the information that is the subject of the denial to the Department Head/Designee.

Department Head/Designee

1. If a review of the denial is requested, arranges for a review to be conducted expeditiously, and within 10 working days by someone who was not involved in the initial review.
2. Informs the County Privacy Officer of the results of the review by the Department Head/Designee.

Privacy Officer

1. Informs the requestor of the results of the review by the Department Head/Designee. (If access is granted, refer to "If Access Request is Granted.")
2. Files all completed Requests and Responses in the Department's HIPAA compliance file. Does *not* file with the individual clinical record.

Appendices:

- Request for Access to Health Information Form
- Response to Request for Access to Health Information Form
- Request for Reconsideration of Denial of Access to Health Information Form
- Decision on Reconsideration of Denial of Access to Health Information Form
- Request for Second Reconsideration of Denial of Access to Health Information Form
- Request for Access Tracking Information Form

Request for Access to Health Information

County of Ulster

Department Name_____
Address_____
Department Privacy Officer/Designee: (Name) _____
Phone: _____

As required by the Health Information Portability and Accountability Act (HIPAA), you have a right to request the opportunity to inspect and copy health information that pertains to you. Department will evaluate your request and will either grant it or explain the reason why the request will not be granted. Your right to access does not extend to information compiled in reasonable participation of, or for use in, a civil, criminal, or administrative action or proceeding, or to information we received in confidence from someone other than another health care provider.

I hereby request access to health information for:

_____
_____.
(Print individual's name and address)

If known: Year of birth: _____

SCOPE OF ACCESS REQUESTED

I would like access to: ☐ All of the records ***or***
☐ The portion of the records concerning:

_____
_____
_____
_____
(Specify the information or portion of records in which you are interested.)

TYPE OF ACCESS REQUESTED

☐ Inspection. Please let me know when I may come to inspect the records. I understand that the Privacy Officer or another employee will be present and that I may not make any marks or alter the records in any way.
☐ Copies. I would like copies of all records requested. Please inform me of any charges for copying records.
☐ I would like the information in the following form or format:

_____

☐ I would like the copies sent directly to the following person:
Name: _____
Address: _____

CHARGES

Inspection. I understand that I may not inspect my records alone. I realize that **Department Privacy Officer/Designee** will accompany me while I inspect my records and that at no time will I be permitted to be alone with my records.

Copies or Transfer. I understand that you may charge me a reasonable cost based fee for copies or the agreed upon charge for copies electronic media format. I understand that you cannot deny me either i) access to my records, or ii) copies of my records, solely because I am unable to pay your costs.

☐ I hereby agree to pay the charges for copying as specified above.
☐ Please call me to let me know the total cost that I will incur.
☐ I am unable to pay for the copies.

Signed: _____ **Date:** _____

Print Name: _____ **Telephone:** _____

If not signed by the individual, please indicate relationship: _____

Name of Individual: _____

Response to Request for Access to Health Information

Department Name_____
Address_____
Department Privacy Officer/Designee: (Name) _____
Phone: _____

Dear _____:

We received your request for access to your health information / the health information of _____.
(Individual's name and address)

☐ **Your request is granted.**
- ☐ You may come in and inspect the records on _____
- ☐ We will send the copies you requested within 10 working days of the date of this notice.
- ☐ The cost for copying the requested records is _____. Please arrange for payment with the Department. **(Phone: _____)**
- ☐ As you requested, the copies will be sent directly to:
  Name: _____
  Address: _____

☐ **Your request is denied**.
- ☐ The Department does not have the records requested.
  - ☐ The information you requested is located at: _____
    _____
    (Address or other contact information).
  - ☐ This Department does not know where the requested information is located.
- ☐ The records requested were compiled in reasonable anticipation of or for use in a civil, criminal, or administrative action or proceeding.
- ☐ You are not allowed by law to access these records.

Sincerely,

_____

_____ _____
Print Name *Date*

NOTE: *If you believe your rights have been violated, you may file a complaint with Department Head or with the Secretary of the Department of Health and Human Services. All complaints must be submitted in writing to our Privacy Officer at the address listed at the top of this form. You will not be penalized for filing a complaint. A complaint form is available from the Privacy Officer listed above.*

Request for Reconsideration of Denial of Access to Health Information

Department Name_____
Address_____
Department Privacy Officer/Designee: (Name) _____
Phone: _____

I understand that my request for access to the records of_____
(Name of Individual)
dated_____was denied.

I request that this denial be reconsidered by another Designee who did not participate in the original decision to deny my request.

Signed:_____**Date:** _____

Print Name:_____**Telephone:** _____

If not signed by the individual, please indicate relationship: _____

Name of Individual: _____

Decision on Reconsideration of Denial of Access to Health Information

Department Name_____
Address_____
Department Privacy Officer/Designee: (Name) _____
Phone: _____
Dear _____:

We received your request for reconsideration of our denial of access to the health information of _____.
(*Name of Individual*)

Upon reconsideration, your request:

___is still denied.
___is granted.

You may come in and inspect the records on _____
(date and time within ten (10) working days after receipt of request)

We will generally send the copies you requested within 10 working days of the date of this notice.

Sincerely,

_____

_____ _____
Print Name *Date*

NOTE: *If you believe your rights have been violated, you may file a complaint with Department or with the Secretary of the Department of Health and Human Services. All complaints must be submitted in writing to our Privacy Officer at the address listed at the top of this form. You will not be penalized for filing a complaint. A complaint form is available from the Privacy Officer listed above.*

Request for Access Tracking Information

DEPARTMENT

Name of Individual:_____

For Office Use Only:

Date received:	Processed by:
Review Date:	Response Date:
Individual Follow-up:___Yes __ No	Date of Individual Follow-up:
Department Follow-up:___Yes __ No	Date of Department Follow-up:
Reconsideration Request: __ Yes___No	Date of Reconsideration Request:
Department Follow-up:___Yes __ No	Date of Department Follow-up:

Reviewer's Comments: *(Please date and sign all entries.)*

_____

_____

_____

_____

Action Taken: *(Please date and sign all entries.)*

_____

_____

_____

_____

Procedure: *HIPAA/HITECH Compliance*
Topic: *Amendment Requests*

HIPAA Regulation:

- *Amendment* § 164.526

Purpose:

The purpose of this procedure is to provide individuals with the opportunity to amend incorrect health information in accordance with the HIPAA requirements.

Procedure Description:

It is the procedure of **County of Ulster** that all requests for amendment of incorrect protected health information maintained by this organization will be considered in a timely fashion. If such requests demonstrate that the information is actually incorrect, County of Ulster will allow amending language to be added to the appropriate document and this addition will be done in a timely manner.

It is also the procedure of the County of Ulster that notice of such corrections will be given to any organization with which the incorrect information has been shared. Under no circumstance, however, is original health information to be written over, obliterated in any way, or otherwise adulterated. All amendments will be made on a specific form designed for the purpose of amending health information only.

Procedure Responsibilities:

Staff

1. Forwards all requests for amendment to the Department Privacy Officer/Designee.

Department Privacy Officer/Designee

1. Contacts the individual (or his/her personal representative) who has requested an amendment within 10 working days of the request.
2. Informs the individual (or his/her personal representative) that the request for amendment must be submitted using the Request for Amendment form.
3. Provides the form in person, by mail, or by fax. Assists in completing the form, if requested.
4. Tracks the status of each request in the tracking information section of the Request for Amendment form.
5. Schedules a time for the individual (or his/her personal representative) to visit the Department and inspect the clinical record, if needed.

6. Reviews the amendment information stated on the Request for Amendment form.
7. Meets with the appropriate program director/supervisor to review the amendment, if necessary.
8. Determines whether to accept or deny the amendment. (See NOTE below)
9. Records the decision in the response section of the Request for Amendment form.
10. Forwards a copy of the response section of the Request for Amendment form to the individual (or his/her personal representative) within 10 working days of completion, by certified receipt requested mail. (*HIPAA requires that action is taken on the amendment within 60 days of receiving the written request*.)
11. Completes the tracking information section of the Request for Amendment form.

NOTE: An amendment may be denied only for one of the following four reasons:

- **The information is accurate and complete as it is,**
- **The information did not originate at this organization,**
- **The information is not part of a set of records for making decisions about the individual, or**
- **The information is not available for inspection for some other reason.**

If Amendment Request is Accepted:

Department Privacy Officer/Designee

1. Inserts the amendment into the clinical record in a special section or tab titled "Amendments".
2. Places an **Amendment** label on the front of the record indicating that an amendment is in place.
3. Sends a copy to the individuals or entities that the individual or the individual's personal representative has requested to be notified (if any).
4. Sends a copy of the amendment to any other entities or business associates who may have received the incorrect information.
5. Notifies appropriate staff of the amendment to ensure that accurate information is disclosed from this point forward.
6. Files the original request and the response in the Department's HIPAA compliance file.

If Amendment Request is Denied:

Department Privacy Officer/Designee

1. Ensures that the denial of amendment includes a statement of the requestor's rights:
    a. To request that the proposed amendment be included in all future disclosures.
    b. To file a statement of disagreement (a template is included in the statement of disagreement section of the Request for Amendment form).
    c. To complain to the Department or to the Department of Health and Human Services.

2. Files the original request and the response in the Department's HIPAA compliance file unless the requestor asks that they be filed with the requestor's clinical record, in which case files them with the requestor's clinical record.
3. Files the individual's statement of disagreement (if any) in the clinical record.
4. If appropriate, composes a rebuttal using the rebuttal section of the Request for Amendment form and files it with the statement of disagreement. Provides a copy of the rebuttal to the requestor**. (Department is not required to file a rebuttal. However, if it does, it *is* required to provide a copy to the requestor.)**

Appendices:

- Request for Amendment of or Addition to Protected Health Information Form
- Response to Request to Amend Protected Health Information Form
- Response to Rejection of Amendment Request Form
- Amendment or Addition Tracking Information Form

Request for Amendment of or Addition to Protected Health Information

County of Ulster

Department Name_____
Address_____
Department Privacy Officer/Designee: (Name) _____
Phone: _____

As required by the Health Information Portability and Accountability Act, you have a right to request that health information that pertains to you be amended if you believe that it is incorrect or incomplete. Department will review your request and either grant your request or explain the reason why it will not be granted. In the event that your request is not granted, you have the right to submit a statement of disagreement that will accompany the information in question for all future disclosures.

I,_____(*print name*), believe that the following health information pertaining to me (or the individual identified below) is incorrect or incomplete (please explain below or attach the challenged entry and identify its location in the clinical record):

_____
_____
_____
_____
_____

I believe that the information described above is incomplete or incorrect for the following reasons:

_____
_____
_____
_____
_____

I hereby request that you amend the health information identified above as follows:

_____
_____
_____
_____

In addition, I request that the following people be notified of the correction:

Name	Address
_____	_____
_____	_____
_____	_____
_____	_____

Department will not make the requested changes if:

1. ***They do not involve your clinical records, billing records, or other records that we use to make decisions about you; or***
2. ***They involve records that you do not have the right to access; or***
3. ***We did not create the information (unless the person or entity that created the information is unable to act on your request); or***
4. ***The information is already accurate and complete.***

If Department agrees to change your information, they will communicate the changed information to the persons or entities that you have designated above. They will also communicate the changed information to any other persons or entities that they know have received the information before it was amended. If they are not able to act on this request in 60 days, they will notify of the reasons for the delay.

Signed: _____ Date: _____

Print Name: _____ Telephone: _____

If not signed by the Individual, please indicate:

Relationship:

- ☐ Parent or guardian of individual
- ☐ Health Care Proxy or Agent
- ☐ Beneficiary or personal representative of deceased individual
- ☐ Other (specify) _____

Name of Individual: _____

Response to Request to Amend Protected Health Information

County of Ulster

Department Name_____
Address_____
Department Privacy Officer/Designee: (Name) _____
Phone: _____

Dear_____:

We received your request to change your clinical information (or the clinical information of the individual listed below) dated_____, and have the following response:

☐ We will make the change you requested and notify the people you listed of the change.
☐ We need more time, and will send you a response by_____. [*Date that is no later than ninety (90) days after our receipt of your request*]
☐ We will grant your request in part, and make the following change:

_____
_____
_____
_____

☐ We will not make the change you requested. If we did not make the change, or the entire change you requested, it was because:

- ☐ The information you want changed is not part of your medical or billing records, or other records which we use to make decisions about you.
- ☐ You do not have the right to access the information you want changed.
- ☐ We did not create the information you want changed, and have no reasonable basis to believe the person who created the information cannot act on your request.
- ☐ The information is already accurate and complete.
- ☐ Other _____
  _____
  _____

If we denied your request in whole or in part, you may request that we include with all future disclosures of the contested information either a "Statement of Disagreement" or a copy of your request for amendment and our denial.

If you want to submit a "Statement of Disagreement" or if you want us to include your request for amendment and our denial with future disclosures of this information, please complete the attached form and return it to us.

Sincerely,

_____ _____
Title

_____ _____
Print name *Date*

NOTE: *If you believe your rights have been violated, you may file a complaint with Department or with the Secretary of the Department of Health and Human Services. All complaints must be submitted in writing to our Privacy Officer at the address listed at the top of this form. You will not be penalized for filing a complaint. A complaint form is available from the Privacy Officer listed above.*

Response to Rejection of Amendment Request

County of Ulster

Department Name_____
Address_____
Department Privacy Officer/Designee: (Name) _____
Phone: _____

I understand that my request for amendment of my medical records dated_____was denied.

Please choose only one of the following:

1. STATEMENT OF DISAGREEMENT

☐ I want the following statement of my disagreement with your denial of my request for amendment of my information to be included with all future disclosures of the contested clinical information. I disagree with the denial because:

_____
_____
_____
_____

I understand that you may distribute a rebuttal to this Statement of Disagreement, and that if you write a rebuttal you will send me a copy.

2. REQUEST FOR INCLUSION OF MY REQUEST FOR AMENDMENT AND YOUR DENIAL

☐ I want my request for amendment and your denial notice to be included with all future disclosures of the contested information.

Signed:_____ Date:_____

Print Name:_____Telephone: _____

If not signed by the individual, please indicate:

Relationship:

- ☐ Parent or guardian of individual
- ☐ Health Care Proxy or Agent
- ☐ Beneficiary or personal representative of deceased individual
- ☐ Other (specify)_____

Name of Individual: _____

Amendment or Addition Tracking Information

County of Ulster

Department Name_____
Address_____
Department Privacy Officer/Designee: (Name) _____
Phone: _____

Name of Individual: _____

Address: _____

_____

For Office Use Only:

Date received:	Processed by:
Review Date:	Response Date:
Individual Follow-up:__ Yes____No	Date of Department Follow-up:
Individual Follow-up: __ Yes____No	Date of Department Follow-up:

Reviewer's Comments: (Sign and date all comments.)

_____
_____
_____
_____

Action Taken: (Sign and date all entries.)

_____
_____
_____
_____

Procedure: HIPAA/HITECH Compliance
Topic: *Assigned Privacy Responsibility*

HIPAA Regulation:

- *Administrative Requirements* § 164.530

Purpose:

At all times, **County of Ulster** shall have one individual identified and assigned to HIPAA privacy responsibility.

Procedure Description:

The HIPAA Privacy Officer is responsible for the oversight of Privacy Rule implementation by departments with HIPAA covered components. The Privacy Officer is responsible for:

1. The development and implementation of the privacy policies and procedures of the Organization
2. The receipt of privacy complaints
3. The provision of further information about matters covered by the Notice of Privacy Practices
4. To act as a single point of contact for all issues related to HIPAA privacy

Responsible Parties:

HIPAA Security Officer
HIPAA Privacy Officer

Procedure: *HIPAA/HITECH Compliance*
Topic: *Complaint Processing*

Purpose:

The purpose of this procedure is to provide guidance for the handling of privacy complaints.

Description:

It is the procedure of **County of Ulster** that all complaints regarding actual or potential violations of an individual's privacy rights will be referred to the Privacy Officer for investigation, follow-up, and corrective action.

Actions To Be Taken For All Complaints

FOLLOW THIS PROCEDURE EXACTLY AS IT IS WRITTEN. IF, FOR ANY REASON, YOU CANNOT PERFORM EACH OF THESE STEPS AS DIRECTED, CONTACT THE PRIVACY OFFICER BEFORE CONTINUING.

1. Staff will inform his/her supervisor immediately whenever he/she receives a privacy complaint from an individual or the individual's personal representative. The supervisor will immediately report the complaint to the Privacy Officer by phone and include, at a minimum:

   - the name of the complainant;
   - the date and time of the complaint; and
   - the name of the staff member who received the complaint.

   If the complaint is made in person to the supervisor, he/she will request that the complainant complete a Complaint Form.

2. In addition to these reporting steps, within 10 working days after receiving the complaint, the supervisor will send a written memo to the Privacy Officer to document the fact that a complaint was made. If the complaint was made in person and the complainant completed a Complaint Form, the Form will be forwarded to the Privacy Officer.

3. The Privacy Officer will contact the individual making the complaint within 10 working days of receiving the initial notice from the staff. The most efficient and immediate means available, preferably verbally by telephone, will be used to contact the individual. The date and time of his/her response will be documented. If a voice mail is left, the Privacy Officer will continue to pursue direct communication until it occurs.

The Privacy Officer will request that the individual complete the Complaint Form (if the original complaint was verbal or written in non-standard format). This form can be mailed to the individual after the initial conversation. If the individual refuses to complete the Complaint Form, the Privacy Officer will complete the Complaint Form and note the refusal on the form.

4. The Privacy Officer will file the completed Complaint Form in the HIPAA Complaint file and not as part of the individual's clinical record.

Actions To Be Taken When No Compliance Violation Is Found

THIS PROCEDURE MUST BE FOLLOWED EXACTLY AS IT IS WRITTEN.

1. If the Privacy Officer determines that there has been no violation of the County of Ulster's privacy policies, the finding will be documented on the complaint form. (*IMPORTANT: If, in the course of investigating the privacy complaint, the Privacy Officer determines that the complaint is related to clinical or medical care or a reportable incident, the situation will be immediately reported to the Department Head/Designee and the County of Ulster's Insurance Department, if applicable, as an incident.)*

2. The Privacy Officer will meet with the individual and explain the findings; the individual will be provided with a written record of the complaint resolution.

3. The Privacy Officer will document the complainant's response (whether they are satisfied or dissatisfied with the disposition of the complaint) on the Complaint Form.

4. If the individual is dissatisfied with the disposition of his or her complaint, the Privacy Officer will refer the matter to:

   - County of Ulster's Insurance Department as part of their early warning program;
   - County of Ulster's legal counsel for compliance related matters; and
   - The County Executive's Office.

Actions To Be Taken When A Compliance Violation Is Found

THIS PROCEDURE MUST BE FOLLOWED EXACTLY AS IT IS WRITTEN.

1. If the Privacy Officer determines that a violation of County of Ulster's privacy procedures has occurred, this fact will be documented on the Complaint Form.

2. The Privacy Officer will meet with the County Executive's Office and appropriate Department Heads(s) within 10 working days to review the violation and develop a remediation plan. The Privacy Officer will document the remediation steps on the Complaint Form and the action plan established to complete them. The Privacy Officer will advise the appropriate workforce members or other persons (if any) who bear responsibility for privacy policy violations and confer with the County Executive's designee and appropriate Department Head(s) to impose the appropriate disciplinary measures on responsible personnel. (*IMPORTANT: If, in the course of investigating the privacy complaint, the Privacy Officer determines that the complaint is related to clinical or medical care or a reportable incident, the situation will be immediately reported to the County Executive's Office and the County of Ulster Insurance Department as an incident, if applicable.)*

3. The Privacy Officer will meet with the individual and explain the findings; the individual will be provided with a written record of the complaint resolution.

4. The Privacy Officer will document the complainant's response (whether they are satisfied or dissatisfied with the disposition of the complaint) on the Complaint Form.

5. If the individual is dissatisfied with the disposition of his or her complaint, the Privacy Officer will report this matter to:

    - County of Ulster's Insurance Department as part of their early warning program;
    - County of Ulster's legal counsel for compliance related matters; and
    - The County Executive's Office.

6. The Privacy Officer will report to the County Executive's Office designee on a weekly basis to report the status of the remediation plan until all corrective activities have been accomplished.

Appendices:

- Complaint Form
- Response to Complaint Form
- Complaint Tracking Information Form

Complaint Form

County of Ulster

Department Name_____
Address_____
Department Privacy Officer/Designee: (Name) _____
Phone: _____
Ulster County Privacy Officer: (Name)_____**Phone:** _____

As required by the Health Information Portability and Accountability Act (HIPAA), you have a right to complain about our privacy policies, procedures, or actions. The County of Ulster will not engage in any discriminatory or other retaliatory behavior against you because of this complaint. Please be as thorough and forthright as possible, and return this form to our Privacy Officer listed above.

Please complete the sections below:

Name:
Address:
Phone:
E-mail Address:
What is the best way to reach you?
What are the best hours to reach you?

Details of your complaint: *(Please be as specific as possible with dates, times, and the specific policy, procedure, or action taken; include the names, if any, of anyone in the County of Ulster with whom you discussed this. Use the other side of this form if you need more room. Attach any documents that you believe pertain to this complaint.)*

___ Documents are attached (describe below):

Signed:_____Date:
_____

Print Name:_____Telephone:
_____

If not signed by the individual, please indicate:

Relationship:

- ☐ Parent or guardian of individual
- ☐ Health Care Proxy or Agent
- ☐ Beneficiary or personal representative of deceased individual
- ☐ Other (specify)

Name of Individual: _____

Response to Complaint

County of Ulster

Department Name_____
Address_____
Phone: _____

Ulster County Privacy Officer: (Name)_____**Phone:** _____

Dear_____:

Action on your complaint, dated_____(attached) has been completed.

We have investigated your concern and have concluded the following:
Findings:

_____

_____

_____

We have taken the following steps to reduce any harm you may have suffered:

_____

_____

_____

We have taken the following steps to reduce the likelihood this will happen again:

_____

_____

Sincerely,

_____

_____ _____
Print name *Date*

NOTE: *If you believe your rights have been violated, you may file a complaint with* ***the County of Ulster Compliance Officer*** *or with the Secretary of the Department of Health and Human Services. All complaints with the County of Ulster must be submitted in writing to our Privacy Officer at the address listed at the top of this form. You will not be penalized for filing a complaint*.

County of Ulster
Privacy Officer
Complaint Tracking Information

Name of Individual: _____
Address: _____
_____

Department/Program: _____

Date received:	Processed by:
Review Date:	Response Date:
Complainant Follow-up: Yes No	Date of Follow-up:

Reviewer's Comments: (Sign and date each comment)

_____
_____
_____
_____
_____
_____

Action Taken: (Sign and date each activity)

_____
_____
_____
_____
_____
_____

Procedure: *HIPAA/HITECH Compliance*
Topic: *Disclosure Accounting Request Processing*

HIPAA Regulation:

- *Disclosure Accounting* § 164.528

Purpose:

The purpose of this policy is to provide individuals an accounting of disclosures of protected health information in accordance with the HIPAA requirements.

Procedure Description:

It is the procedure of **the County of Ulster** that an accounting of all disclosures subject to such accounting of protected health information (PHI), in accordance with the Health Information Portability and Accountability Act (HIPAA), be provided to individuals or their personal representatives whenever such an accounting is requested.

Policy Responsibilities:

Department Staff

1. Forwards all requests for disclosure accounting to the Department's Privacy Officer**.**

Department's Privacy Officer/Designee

1. Contacts the individual or personal representative who requests a disclosure accounting within five business days of the request.
2. Informs the individual or his/her personal representative that the County of Ulster requires the request to be documented and submitted using the Request for Accounting of Disclosures of Protected Health Information form.
3. Provides the requestor with a copy of the form, offering assistance as necessary.
4. Reviews Request for Accounting of Disclosures of Protected Health Information form, verifying that the accounting is valid and includes only health information disclosures that are required to be accounted for by HIPAA. (See NOTE below)
5. Reviews the request to determine if a law enforcement official has requested that disclosures to the law enforcement organization not be included in an accounting of disclosures at this time. (If so, omits the relevant disclosures from the disclosure accounting.)
6. Reviews the records and compiles a list of every disclosure for the period of six years prior to the date of request subject to an accounting.

7. Ensures that each entry contains:
    a. The date of the disclosure.
    b. The name of the entity or person who received the protected health information and, if known, the address of such entity or person.
    c. A brief description of the protected health information disclosed.
    d. A brief statement of the purpose for each disclosure.
8. If many disclosures were made to the same entity for the same purpose, it is permissible to group them together by providing the following:
    a. The information identified above.
    b. How frequently or how many times the information was disclosed.
    c. The date of the last such disclosure.
9. Provides the completed Accounting of Disclosures form to the individual or personal representative.
10. Files the request and the completed Request for Accounting of Disclosures form in the Department's HIPAA compliance file.

NOTE:

The following disclosures of PHI are not subject to an accounting:

- Disclosures made to carry out treatment, payment, and health care operations.
- Disclosures made to the individuals about them.
- Disclosures made to persons involved in the individual's care.
- Disclosures made for national security or intelligence purposes.
- Disclosures made to correctional institutions or law enforcement officials.
- Disclosures that are incident to a permitted use or disclosure.
- Disclosures made pursuant to an authorization.
- Information in the facility's directory.
- Information as part of a limited data set.

Appendix: Request for Accounting of Disclosures of Protected Health Information Form

Request for Accounting of Disclosures of Protected Health Information

County of Ulster

Department Name_____
Address_____
Department Privacy Officer/Designee: (Name) _____
Phone: _____
Ulster County Privacy Officer: (Name)_____**Phone:** _____

As required by the Health Insurance Portability and Accountability Act, you have a right to request an accounting of disclosures of health information that pertains to you.

REQUEST SECTION

I,_____(print name), hereby request an accounting of disclosures of protected health information pertaining to me (or the individual identified below) that have occurred over the last six (6) years.

Signed: _____Date: _____
Print Name:_____ Telephone: _____
If not signed by the Individual, please indicate:

Relationship:

- ☐ Parent or guardian of individual
- ☐ Health Care Proxy or Agent
- ☐ Beneficiary or personal representative of deceased individual (i.e., parent, guardian, healthcare proxy, etc.)
- ☐ Other (specify) _____

Name of Individual: _____

REQUEST PROCESSING SECTION

This section is to be completed by the reviewer:

Date received:	**Reviewed by:**
Dept. Privacy Officer:	**Review Date:**

The requested disclosure accounting was processed on_____(Date)

_____ _____
Print Name Title

_____ _____
Signature Date

Policy and Procedure: *HIPAA/HITECH Compliance*
Topic: *Individual Authorization for Disclosure*

HIPAA Regulation:

- *Authorizations* § 164.508

Purpose:

The purpose of this policy is to assure authorizations for use or disclosure of protected health information in accordance with the HIPAA requirements.

Procedure Description:

It is the procedure of **County of Ulster** that a valid authorization will be obtained for all disclosures that are not for treatment, payment, or health care operations, to the individual or their personal representative, to persons involved with the individual's care, to business associates in their legitimate duties, or for public purposes. This authorization will include all the mandatory elements and any authorizations generated from outside will be reviewed by the Department's Privacy Officer to verify that they are valid.

Policy Responsibilities:

Department Staff

1. Obtains blank Authorization for the Use or Disclosure of Protected Health Information form.
2. Confirms the identity of the person who will sign the authorization (if not known). (If the person who will sign the authorization is a personal representative, i.e., guardian, health care proxy, family member, advocates, etc., confirms his or her relationship to the individual.)
3. Completes all parts of the authorization form that need to be completed and obtains required signatures. Does not leave any line blank.
4. Provides a copy of the signed authorization to the individual or personal representative.
5. Files a copy of the signed authorization in the client's record.
6. Where feasible, seeks the individual's verbal agreement to release or disclose Protected Health Information (PHI) to a family member or friend involved in the individual's care **before each such disclosure**.
7. If the individual provides verbal agreement, documents this client's record.
8. Records verbal agreement in the HIPAA section. Includes the date, time, name, and telephone number of the family member or friend in the record, as appropriate. Staff member must sign and date the entry.

9. Does not discuss or disclose any information pertaining to the individual to any person who has not been granted specific, documented permission.
10. If the Authorization for the Use or Disclosure of Protected Health Information form was created by an outside provider or agency, forward the Authorization Form to the Department's Privacy Officer/designee for review.

Department's Privacy Officer/Designee

1. Reviews the Authorization for the Use or Disclosure of Protected Health Information form to assure the following information is present:
    a. A description of the information to be used or disclosed.
    b. The person(s) authorized to make the requested use or disclosure.
    c. The person(s) to whom the disclosure will be made.
    d. The purpose of the disclosure (Note: "At the request of the individual" is permissible).
    e. An expiration date or event.
    f. A statement of the individual's right to revoke the authorization.
    g. Dated signature of the individual (if signed by a personal representative, a description of the representative's authority to act for the individual should be included).
    h. A statement that authorization is not a condition of treatment, payment, or eligibility for benefits.
    i. A statement that information disclosed pursuant to the authorization may be further re-disclosed and no longer protected by HIPAA.

Appendix: Authorization for the Use or Disclosure of Protected Health Information Form

Authorization for the Use or Disclosure of Protected Health Information

County of Ulster

Department Name_____
Address_____
Department Privacy Officer/Designee: (Name) _____
Phone: _____
Ulster County Privacy Officer: (Name)_____Phone: _____

As required by the Health Insurance Portability and Accountability Act, County of Ulster may not use or disclose your health information except as provided in our Notice of Privacy Practices without your authorization. Your signature on this form indicates that you are giving permission for the uses and disclosures of protected health information described herein. You may revoke this authorization at any time by signing and dating the revocation section on your copy of this form and returning to this office.

AUTHORIZATION SECTION

I,_____(print name) hereby authorize the <use / disclosure / use and disclosure> of the following health information that pertains to me:

_____

_____

for the following purpose:

_____

_____

I authorize the following persons to make these disclosures of my health information:

_____

_____

I authorize the following persons to receive these disclosures of my health information:

_____

I understand that information disclosed pursuant to this authorization may be re-disclosed to additional parties and will no longer be protected.

I understand that I may revoke this authorization at any time by signing the revocation section of my copy of this form and returning it to Department_____. I further understand that any such a revocation does not apply to the extent that persons authorized to use or disclose my health information have already acted in reliance on this authorization.

I understand that this authorization will automatically expire on: _____
(must include a date or event).

I understand that I am under no obligation to sign this authorization. I further understand that my ability to obtain services will not depend in any way on whether I sign this authorization or not. I understand that I have a right to inspect and to obtain a copy of any information disclosed pursuant to this authorization.

Print Name: _____

_____ _____
Signature Date

REVOCATION SECTION

I hereby revoke this authorization.

_____ _____
Signature Date

Policy and Procedure: *HIPAA/HITECH Compliance*
Topic: *Information Disclosures*

HIPAA Regulation:

- *Use and Disclosures* — § 164.502, §164.504, §164.506, §164.508, §164.510, §164.512, §164.514

Purpose:

The purpose of this policy is to provide guidance in the use and disclosure of protected health information in accordance with the HIPAA requirements.

Procedure Description:

It is the procedure of **the County of Ulster** to make routine and non-routine disclosures of protected health information (PHI) in accordance with applicable state law and the Health Information Portability and Accountability Act (HIPAA).

Where required by law, the Department will disclose only the minimum information necessary to accomplish the purpose of the disclosure.

Responsibilities:

Department's Privacy Officer/Designee

1. Determines whether or not the disclosure requires an authorization by the individual or the individual's personal representative (i.e., parent, guardian, healthcare proxy, etc.). **All disclosures except the following require an authorization:**
    a. For treatment, payment, or health care operations.
    b. To the individual or to a personal representative of the individual.
    c. To demonstrate compliance with HIPAA regulations (cooperation with the Department of Health and Human Services when it conducts compliance reviews or investigates complaints).
    d. To cooperate with courts, public health authorities, law enforcement agencies, or for other "public purposes".
2. If the disclosure is pursuant to an authorization by the individual or his/her personal representative, ensures the authorization is valid. To be valid, an authorization must include:
    a. A description of the information to be disclosed.
    b. Department is specifically named as authorized to disclose the information.

   c. The name of the person or organization specifically authorized to receive the information.
   d. A description of the purpose for which the information will be disclosed.
   e. An expiration date or expiration event.
   f. Signature of the individual to whom the information pertains. (The signature of the personal representative must include the relationship to the individual.)
   g. The date on which the authorization was signed.
3. Discloses only the minimum amount of information necessary to accomplish the purpose of the disclosure. NOTE: The “minimum necessary” rule does not apply to the following:
   a. Uses or disclosures for treatment purposes.
   b. Disclosures to the Department of Health and Human Services for compliance review or complaint investigation purposes.
   c. Disclosures to the individual or his/her personal representative concerning information that pertains to the individual.
   d. Disclosures authorized by the individual.
   e. Disclosures that are required by law.
   f. Disclosures necessary for HIPAA compliance.
4. Confirms the identity of the party (if not known) before the disclosure is made.
5. If the disclosure is "accountable", records the disclosure on the Disclosure Tracking Log. The following disclosures are not “accountable”:
   a. Disclosures for the purpose of treatment, payment, and health care operations.
   b. Disclosures made to the individual or to personal representatives of the individual.
   c. Disclosures that were authorized by the individual (or the individual's personal representative).
   d. Disclosures made for national security or intelligence purposes.
   e. Disclosures made to correctional institutions or law enforcement officials.
   f. Disclosures of limited data set information.
   g. "Incidental" disclosures (defined as unintended disclosures that cannot reasonably be prevented, are limited in nature, and that occurs as a result of another use or disclosure that is permitted by HIPAA).
   h. Disclosures that occurred prior to April 14, 2003.
6. Consults Department’s Privacy Officer if assistance or direction is needed.

Actions To Be Taken When Disclosing Information to Law Enforcement, Public Authorities, Disclosing Information For A Judicial Or Administrative Proceeding and Disclosing Information About Deceased Individuals

Department’s Privacy Officer/Designee

1. Immediately notifies Department Head of any requests for information by law enforcement officials.

2. Contact Ulster County Privacy Officer/First County Attorney.

3. Records the disclosure on the Disclosure Tracking Log

Actions To Be Taken When Disclosing Information To The Department Of Health and Human Services as Part Of A Compliance Review

The County of Ulster will cooperate fully with the Department of Health and Human Services (DHHS) when conducting compliance reviews. Employees will answer all questions of DHHS compliance investigators and provide access to DHHS personnel to all requested records.

Appendix: Protected Health Information Disclosure Tracking Log

Department _____
Protected Health Information (PHI) Disclosure Tracking Log

Consumer Name_____

Date Disclosed	Site/Program	Name of Person/Entity PHI Disclosed to	Authorization Or Written Request? *	Purpose	PHI Disclosed	Disclosed by

* If so, please attach.

Procedure: *HIPAA/HITECH Compliance*
Topic: *Marketing*

HIPAA Regulation:

Marketing	§ 164.501 § 164.508(a)(3)

Purpose:

The purpose of this procedure is to ensure that **ORGANIZATION** is in compliance with HIPAA's requirements regarding marketing.

Procedure Description:

It is the procedure of **County of Ulster** to safeguard the confidentiality and integrity of Protected Health Information (PHI) and to protect against the unauthorized access to, or release of such information.

It is also the procedure of **County of Ulster to** ensure compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) requirements regarding marketing. HIPAA prohibits the use or disclosure of an individual's PHI for marketing purposes unless the marketing communication is directly related to treatment of the patient, describes treatment alternatives, is for case management or care coordination, made face-to-face with the patient, or it involves a promotional gift of nominal value

Departments will not use or disclose an individual's PHI for marketing purposes without the patient's written authorization.

Responsibilities:

Department Head

1. Determines whether or not the proposed activity or communication requires an authorization by the individual or the individual's personal representative. **All uses or disclosures except the following require an authorization:**
    a. The communication describes a health-related product or service provided by **Department Name**_____that:
        i. for purposes of treating the individual; or
        ii. is for case management or care coordination of the individual (e.g., for directing or recommending alternative treatments, therapies, health care providers, or care settings).
    b. The communication promotes health in a general manner and does not promote a specific product or service.
    c. The communication is used to promote health fairs, wellness classes, support groups, and population-based activities to improve health or reduce health costs.

d. The marketing or communication is conducted in a face-to-face meeting with the individual or personal representative.
e. A promotional gift of nominal value (e.g., a pen with **Program's** name or logo) is given or sent to the individual.
f. Consults Department's Privacy Officer for further guidance.
g. Obtains a valid written authorization from the individual or personal representative before any marketing communication or product is sent to the individual.
h. If **the Department** will receive either direct or indirect remuneration from a third party as a result of the marketing activity, this information will be prominently included in the authorization that the individual or personal representative signs.
i. Provides a copy of the signed authorization to the individual or personal representative.
j. Files the signed authorization in the record.
k. Authorization is maintained for six (6) years.

Procedure: *HIPAA/HITECH Compliance*
Topic: *Privacy Notice and Acknowledgement*

HIPAA Regulation:

- *Notice of Privacy Practices* § 164.520

Purpose:

The purpose of this procedure is to provide guidance with respect to the Notice of Privacy Practices in accordance with the HIPAA requirements.

Procedure Description:

It is the procedure of **County of Ulster** that a Notice of Privacy Practices (the Notice) must be published, that the Notice and any revisions to it must be provided to all individuals at the earliest practical time, and that all uses and disclosures of protected health information (PHI) must be done in accordance with Organization's Notice of Privacy Practices.

It is the policy of the Department that efforts will be made to gain written acknowledgment of the receipt of the Notice from all individuals to whom we provide the Notice of Privacy Practices. If written acknowledgment is not provided**,** the Department will document attempts to gain such acknowledgment. Attempts will include a letter and one phone call to follow-up if there is no response to the letter.

Responsibilities:

Department's Privacy Officer/Designee

1. Maintains the Notice and updates it when changes occur.
2. Maintains all versions of the Notice in the Organization's HIPAA Compliance file.
3. Posts the Notice in the general program areas, administrative office, and residences. Assures the Notice is posted on Ulster County's website.
4. Makes the Notice available in other languages, if appropriate.
5. When the Notice changes, posts the most current Notice. Also posts a sign that indicates that the Notice has been modified and how individuals may receive a copy of the new notice.
6. Provides notification to all programs of any changes to the Notice.

Department's Privacy Officer/Designee

1. Assures that the Notice is provided to all individuals who have not previously been given the Notice.
2. Assures individuals and/or personal representatives (involved family, guardian) are advised to read the Notice and sign the acknowledgment. Assures that assistance is provided to individuals as needed in reading and/or understanding the notice.
3. Provides each individual receiving the Notice with Organization's Acknowledgment of Receipt of Notice of Privacy Practices. (Acknowledgment is a separate page from the Notice.)
4. Assures that the individual's signed acknowledgment is filed in the individual's clinical record in the HIPAA section.
5. When the Notice changes, assures a copy of revised Notice is provided to individuals and/or personal representative (involved family, guardian, advocate, etc.) at the next treatment/service plan review or service encounter, whichever comes first.
6. If the individual refuses to sign the acknowledgment, an offer to contact the Department's Privacy Officer will be made (Treatment/services will not be withheld upon refusal to sign the acknowledgment).

Department's Privacy Officer

1. Answers individual's questions or concerns.

Department Staff

1. Documents the efforts to explain the Notice and subsequent failure to obtain a signature on the Acknowledgement Form.
2. Forwards all requests for special privacy protections, alternate confidential communication channels, amendments to PHI, disclosure accounting, or access to or copying of PHI, and complaints to the Department's Privacy Officer. Staff will communicate all requests described above in writing to the Department's Privacy Officer.

Appendix: Acknowledgement of Receipt of Notice Form

Acknowledgement of Receipt of Notice

County of Ulster

Department Name_____
Address_____
Department Privacy Officer/Designee: (Name) _____
Phone: _____
Ulster County Privacy Officer: (Name)_____**Phone:** _____

I hereby acknowledge that I have received a copy of **Department**_____Notice of Privacy Practices.

Yes No (circle one) I would like to receive a copy of any amended Notice of Privacy Practices at: _____

Signed:_____Date: _____

Print Name:_____Telephone: _____

If not signed by the individual, please indicate relationship:

- ☐ Parent or guardian of individual
- ☐ Health Care Proxy or Agent
- ☐ Beneficiary or personal representative of deceased individual
- ☐ Other

Name of Individual: _____

***For Department Use Only*:**

Signed form received by: _____

Acknowledgment refused:

Efforts to obtain:

_____
_____

Reasons for refusal:

_____
_____

Procedure: *HIPAA/HITECH Compliance* Topic: *Research*

HIPAA Regulation:

- *Research* §164.501, 164.508, 164.512(i) (See also 164.514(e), 164.528, 164.532)

Purpose:

The purpose of this procedure is to describe practices related to the use and disclosure of Protected Health Information for the purpose of research in accordance with the HIPAA requirements. If in the event the County of Ulster would research, as defined by: Research is defined in the Privacy Rule as "a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge." The County will seek legal guidance in the use of disclosure of PHI.

Procedure: *HIPAA/HITECH Compliance*
Topic: *Safeguards for Confidentiality*

Procedure Description:

It is the procedure of **County of Ulster** that all employees, volunteers, and contractors ensure confidentiality and privacy in regard to history, records, and discussions about individuals served. The very fact that an individual is served by this organization must be kept private or confidential; disclosures can be made only under specified conditions and with the appropriate authorization of the individual, the individual's personal representative, or an appropriate Organization representative.

It is the procedure of County of Ulster that (except for disclosures made for treatment purposes) all disclosures of protected health information (PHI) must be limited to the minimum amount of information needed to accomplish the purpose of the disclosure.

It is also the procedure of County of Ulster that all requests for PHI (except requests made for treatment purposes) must be limited to the minimum amount of information needed to accomplish the purpose of the request.

For purposes of this procedure, PHI is defined as any information that is created or maintained by the County of Ulster that relates to the past, present, or future physical or mental health condition of an individual, the provision of care to an individual, or the past, present, or future payment for the provision of care to the individual. It includes any information that identifies the individual or provides a reasonable basis to believe the information can be used to identify the individual. PHI may include, but is not limited to, the individual's name, address, birth date, social security number, benefit information, medical information, service plans, records of treatment or service delivery, and photographs or other images.

The County of Ulster has identified the following safeguards to protect individuals from unauthorized disclosure of PHI.

Verbal Communication
Details concerning individuals, their health information, or information related to service provision should not be discussed in a public area where others may overhear the information. Public areas may include but are not limited to hallways, parking lots, rest rooms, break rooms, and public facilities.

Employees, volunteers, or contractors may not discuss information about individuals served with any unauthorized person, whether on- or off-duty.

Consumer Records/Information
Each employee or contractor is granted access to PHI based on the assigned job functions of the employee or contractor. Such access privileges should not exceed those necessary to accomplish the assigned job function.

All records containing PHI or pertaining to individuals served must be maintained in a secure area, accessible to employees or contractors authorized for such access.

Records stored in general areas must be locked at all times when authorized employees are not in attendance.

Information stored in offices or program areas must be secured and accessible to authorized personnel only.

Employees must maintain a clean desk practice; no PHI may be left unattended on desks or other areas in a manner that is visible to others. Desks and surfaces must be cleared of PHI at the end of the shift/day. Records should be secured in locked drawers or cabinets.

Information pertaining to individuals may not be visibly posted on walls, bulletin boards, etc. This includes but is not limited to rosters, schedules, service needs, and health or medication needs.

Confidential information to be reviewed at meetings shall not be routinely distributed prior to meetings. If it is necessary to distribute confidential information prior to meetings, the following precautions should be observed:

- The material should be clearly marked as confidential;
- Distributed copies of the confidential information should be numbered;
- Each copy should be retrieved at the meeting at which it is reviewed;
- All numbered copies should be destroyed; and
- The original should be retained in a secure location.

Employees or committee members who maintain records of the meetings must assure that the records are safeguarded at all times and that any records are returned to the Organization for destruction or upon separation from the committee or function.

Removal of Records from County of Ulster Premises
Records or information pertaining to individuals may not be removed from the facility without the prior approval of a supervisor with authority over the records.

Employees or contractors will be responsible to sign out any records removed from the facility and complete the documentation upon return of the records.

Employees or contractors are responsible for the safeguarding of records in their possession. No records may be left unattended or unsecured in a manner that will allow access by unauthorized parties.

Employees and contractors must report the loss or destruction of any records to the supervisor with authority over the records immediately upon loss or destruction.

Computer Use and Access
Computer use and access is determined by job functions. Only authorized persons may access the Organization's computers or network.

Employees or contractors may not share passwords or identity with any other person or allow another person access to the computer with their password.

Information Technology personnel must be notified immediately upon the decision to terminate an employee or contractor in order to initiate access restrictions.

Information pertaining to individuals served may not be loaded onto other computer systems without the approval of the Department Head and the appropriate safeguards to prevent unauthorized access or disclosure.

Computer screens should be shielded or located in a manner that prevents access by unauthorized personnel.

Employees or contractors must exit any programs or files containing PHI before leaving the computer unattended. Password protected screensaver should be utilized when computers are unattended.

All e-mail messages must contain a confidentiality statement and include the identity of the County of Ulster's employee or contractor sending the message (See Ulster County's SOP Manual).

No PHI should be emailed outside of the County of Ulster's network unless it is encrypted.

Missing or stolen laptops or other portable devices must be immediately reported to Information Technology personnel.

Fax Protocol
All fax transmissions must include a cover memo including the name and phone number of both the sender and the recipient. All cover memos must include a confidentiality statement.

Employees or contractors who transmit confidential PHI should confirm receipt of the information by the recipient.

Fax machines should be located in a supervised area to prevent unauthorized access or disclosure of confidential information.

Authorized personnel should remove faxes and deliver to the recipient directly or place the document in an interdepartmental envelope for delivery.

Fax machines should be monitored on a routine basis for the receipt of messages.

Printer Protocol
Employees or contractors are responsible for retrieving print jobs containing confidential information promptly upon printing.

Authorized personnel who remove print jobs from a shared printer should deliver the material to the recipient directly or place the information in an interdepartmental envelope for delivery.

Mail Protocol
Personnel are designated by job function to distribute mail within the Departments.

All interagency mail must be placed in an interdepartmental envelope and include the name and department of the recipient and the name and department of the sender.

Employees and contractors are responsible to remove mail from mailboxes on a regular basis. During absences, other personnel should be assigned the responsibility for retrieving and securing the mail.

Employees or contractors should not open the mail of others unless authorized to do so by the appropriate program administrator.

Cellular Phones and Mobile Devices
Mobile devices should not be used to email PHI unless the device has been encrypted and the County of Ulster has authorized such use. Email by its very nature uses an unsecure protocol. There are a number of risks, including the possibility of data interception.

Texting of PHI is prohibited. Text messages are generally not secure because they lack encryption, and the sender does not know with certainty the message is received by the intended recipient. Also, the telecommunication vendor/wireless carrier may store the text messages.

Missing or stolen mobile devices must be reported immediately to Department Head, who will report to Information Services.

Social Media
Employees and contractors are prohibited from posting or including PHI or any information about individuals on social media (i.e., Facebook, YouTube, Twitter).

Procedure: HIPAA/HITECH Compliance
Topic: *Sanctions for Privacy Violations*

HIPAA Regulation:

- *Administrative Requirements* § 164.530

Purpose:

The purpose of this procedure is to ensure that workforce members of **County of Ulster** are informed of sanctions, penalties, and disciplinary actions that may be applied for non-compliance with **County of Ulster**'s HIPAA Privacy Procedures.

Procedure Description:

Workforce members are accountable for their actions in failing to comply with HIPAA Privacy Rule requirements, as defined in **County of Ulster**'s HIPAA Privacy Procedures.

Sanctions
Members of the **County of Ulster** workforce who violate HIPAA Privacy Procedures regarding the safeguarding of protected health information (PHI) are subject to disciplinary action as prescribed by Civil Service or the Collective Bargaining Agreement within the **County of Ulster** up to and including immediate dismissal from employment or service. For violations of these procedures by non-employees, corrective action includes but is not limited to contract cancellation or termination of services.

Members of the **County of Ulster's** workforce who knowingly and willfully violate state or federal law for failure to safeguard PHI are subject to criminal investigation, prosecution, and/or civil monetary penalties.

If **the County of Ulster** fails to enforce privacy and security safeguards, it may be subject to administrative penalties by the federal Department of Health and Human Services Office for Civil Rights, including federal funding penalties.

Reporting Violations
All workforce members shall notify their supervisor who will notify the Department Head who will then notify the Ulster County Compliance Officer when there is a reasonable belief that any privacy and security procedures are being violated.

Retaliation Prohibited

Neither **County of Ulster** as an entity nor any member of **the County of Ulster's** covered workforce shall intimidate, threaten, coerce, discriminate against, or take any other form of retaliatory action against any individual for:

1. Exercising any right established under **County of Ulster**'s HIPAA Privacy Policies and Procedures.
2. Participating in any process established by **the County of Ulster**'s HIPAA Privacy Policy including the filing of a complaint with **the County of Ulster** or with the federal Department of Health and Human Services Office for Civil Rights.
3. Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing relating to the policies and procedures.

Any workforce member who engages in retaliation shall be subject to the sanctions under this policy.

Procedure Responsibilities:

Workforce Member Responsibilities

1. All HIPAA covered workforce members shall comply with **county of Ulster**'s HIPAA Privacy Procedures.
2. All HIPAA covered workforce members shall notify their manager or supervisor or the HIPAA Compliance Officer of their department or division if they have a reasonable belief that any privacy policies or procedures are being violated.
3. All HIPAA covered workforce members are required to sign HIPAA Acknowledgement Form, certifying they have received training on **County of Ulster's** HIPAA Privacy and Security Policies and Procedures, and will comply with the HIPAA Privacy and Security Policies and Procedures.

Procedure: *HIPAA/HITECH Compliance*
Topic: *Workforce Training*

HIPAA Regulation:

- *Training* § 164.530 (b)(1)

Purpose:

The purpose of this procedure is to ensure that the workforce receives the necessary training to comply with **County of Ulster** HIPAA Privacy Policies and Procedures and to prevent any violations of the HIPAA Privacy Rule.

As it relates to this policy, workforce means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for **County of Ulster**, is under the direct control of **County of Ulster**, whether or not they are paid by **County of Ulster**.

Procedure Description:

It is the policy of **County of Ulster** that HIPAA privacy training will be provided to all members of the workforce within a reasonable period of time after the person joins the Organization's workforce.

It is the policy of **County of Ulster** that HIPAA privacy training will be provided to each member of the County of Ulster's workforce whose functions are affected by a material change in the policies or procedures required by the Privacy Rule, within a reasonable period of time after the material change becomes effective.

Responsibilities:

1. The Privacy Officer is responsible for the development and implementation of privacy training courses.
2. Human Resources will be responsible for administering the training program.
3. The workforce training must include training in privacy policies and procedures relating to privacy as implemented by the Organization.
4. The training must be completed within a reasonable period of time after the person joins the County of Ulster's workforce, but not more than 30 days after joining the workforce.
5. For existing members of the workforce whose functions are affected by a material change in the policies and procedures, training must be completed within 365 days of the material change.

Procedure: HIPAA/HITECH Compliance
Topic: *Acceptable Encryption*

Purpose:

The purpose of this procedure is to provide guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively. In addition, this procedure provides direction to ensure that Federal regulations are followed, and legal authority is granted for the dissemination and use of encryption technologies outside of the United States.

Procedure Description / Responsibilities:

Proven, standard algorithms such as Triple DES, Blowfish, Twofish, RSA, and AES should be used as the basis for encryption technologies. These algorithms represent the actual cipher used for an approved application. For example, Secure Socket Layer (SSL) uses RSA encryption. Symmetric cryptosystem key lengths must be at least 56 bits. Asymmetric cryptosystem keys must be a length that yields equivalent strength. In addition, cloud products and services will be FedRAMP compliant. Ulster County's key length requirements will be reviewed annually and upgraded as technology evolves and/or allows.

The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by IT. Be aware that the export of encryption technologies is restricted by the U.S. Government. Residents of countries other than the United States should make themselves aware of the encryption technology laws of the country in which they reside.

Procedure: HIPAA/HITECH Compliance
Topic: *Acceptable Use*

Purpose:

The purpose of this procedure is to outline the acceptable use of information technology equipment at Ulster County. These rules are in place to protect both the employee and Ulster County government. Inappropriate use exposes Ulster County to risks including cyber-attacks, compromise of network systems and services, and legal issues.

This procedure applies to employees, contractors, consultants, temporaries, and other workers at Ulster County.

Description / Responsibilities:

General Use and Ownership

1. Employees are responsible for exercising good judgment regarding the reasonableness of personal use – activities that do not detract from the employees assigned duties and put the County at risk to cyber-attack.
2. Management requires that any information that is considered legally protected, confidential, sensitive or vulnerable be encrypted.
3. For security and network maintenance purposes, authorized individuals within Ulster County may monitor information technology equipment, systems, and network traffic at any time.
4. Ulster County reserves the right to audit networks and systems on a periodic basis to ensure compliance with this procedure.

Security and Proprietary Information

1. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed quarterly; Ulster County Information Services (UCIS) will force user level passwords changes every 90 days. Password complexity rules will be enforced by UCIS as system requirements allow and/or evolve.
2. All desktops, laptops, and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off when the host will be unattended (control-alt-delete keys or Windows logo key + L).
3. Use encryption of information in compliance with the Acceptable Encryption Policy.
4. Information contained on mobile devices and computers is especially vulnerable. Special care should be exercised. All mobile devices and computers shall be encrypted.
5. All hosts used by the employee that are connected to the Ulster County Internet/Intranet/Extranet, whether owned by the employee or Ulster County, shall be continually executing approved virus-scanning software with a current virus database.
6. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain phishing attempts, viruses, malware, and ransomware, etc.

Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of Ulster County authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Ulster County owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of “pirated” or other software products that are not appropriately licensed for use by Ulster County.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Ulster County or the end user does not have an active license is strictly prohibited.
3. Exporting software, technical information, encryption software, or technology in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
4. Introduction of malicious programs into the network or server (e.g., viruses, malware, ransomware, Trojan horses, etc.).
5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
6. Using an Ulster County information technology asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user’s local jurisdiction.
7. Making fraudulent offers of products, items, or services originating from any Ulster County account.
8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For the purposes of this section, “disruption” includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
10. Port scanning or security scanning is expressly prohibited unless prior notification to UCIS is made.
11. Executing any form of network monitoring which will intercept data not intended for the employee’s host, unless this activity is a part of the employee’s normal job/duty.
12. Circumventing user authentication or security of any host, network, or account.
13. Interfering with or denying service to any user other than the employee’s host (for example, denial of service attack).
14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user’s terminal session, via any means, locally or via the Internet/Intranet/Extranet.
15. Providing information about, or lists of, Ulster County employees to parties outside Ulster County government.

Email and Communications Activities

1. Sending unsolicited email messages, including the sending of ‘junk mail” or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone, or paging, whether through language, frequency, or size of messages.
3. Unauthorized use or forging of email header information.
4. Solicitation of email for any other email address, other than that of the poster’s account with the intent to harass or collect replies.
5. Creating or forwarding “chain letters”, “Ponzi”, or other “pyramid” schemes of any type.
6. Use of unsolicited email originating from within Ulster County networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Ulster County or connected via Ulster County’s network.
7. Any discussion or posting of EPHI on social media websites such as Facebook.

Procedure: HIPAA/HITECH Compliance
Topic: *Assigned Security Responsibility*

HIPAA Regulation:

- *Assigned security responsibility* §164.308(a)(2) required

Purpose:

At all times, Ulster County shall have one individual identified and assigned to HIPAA security responsibility.

Description:

The HIPAA Security Officer is responsible for the oversight of Security Rule implementation by departments with HIPAA covered components. Responsibilities are:

1. To ensure that the necessary and appropriate HIPAA security policies are developed and implemented to safeguard the integrity, confidentiality, and availability of electronic protected health information (EPHI) within the HIPAA covered components.
2. To ensure that the necessary infrastructure of personnel, procedures and systems is in place through monitoring, compliance, and providing a mechanism for incident reporting and violations.
3. To act as a single point of contact for all issues related to HIPAA security.

Policy Responsibilities:

HIPAA Security Officer
HIPAA Privacy Officer

Procedure: HIPAA/HITECH Compliance
Topic: *Audit Controls*

HIPAA Regulation:

• *Log-in monitoring*	§164.308(a)(5)	addressable
• *Information system activity review*	§164.308(a)(1)	required
• *Audit controls*	§164.312(b)	required

Purpose:

The purpose of this procedure is to establish the standard of authority to conduct security monitoring and enforce audit controls on computing resources used by HIPAA covered components.

Description:

Ulster County has the requirement to monitor system access and activity of all HIPAA covered component workforce members.

Log-in Monitoring

To ensure that access to servers, workstations, and other information technology systems containing electronic protected health information (EPHI) is appropriately secured, the following log-in monitoring measures shall be implemented:

1. A mechanism to record all failed log-in attempts on network systems containing EPHI when the technology is capable.
2. To the extent that technology allows, a means to disable any User ID that has more than four consecutive failed log-in attempts within a 30-minute period.
3. A review of log-in activity reports and logs when required to identify any patterns of suspicious activity, such as continuous failed log-in attempts.

Information System Activity Review

Information system activity reviews and audits may be conducted to:

1. Ensure integrity, confidentiality, and availability of information and resources.
2. Investigate possible security incidents to ensure compliance with Ulster County Information Technology (IT) and security policies.
3. Monitor user or system activity as required.
4. Verify that software patching is maintained as the appropriate security level.
5. Verify that virus protection is current.

Information System Audit Controls

To ensure that activity for all computer systems accessing EPHI is appropriately monitored and reviewed, these requirements shall be met:

1. Where technology allows, the audit record shall capture sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events.
2. Each fiscal quarter, at a minimum, UCIS support shall review audit logs, activity reports, or other mechanisms for indications of improper use.
3. Indications of improper use shall be reported to management for investigation and follow up.
4. Audit logs of access to networks and applications with EPHI shall be archived and protected from unauthorized access, modification, and deletion.

Procedure Responsibilities:

Information Services Support Responsibilities

1. Implement and manage the log-in monitoring and audit controls through activity reports on systems containing EPHI to comply with the HIPAA Security Rule.
2. Report all suspicious log-in or system activity to management for investigation and follow-up.

Supervisor and Manager Responsibilities

1. Work with UCIS IT support to ensure that user and system activity reports provide sufficient information to determine if improper use of EPHI has occurred.
2. Work with UCIS IT support to investigate reports of potential misuse of log-in accounts or access to EPHI by their workforce.

Procedure: HIPAA/HITECH Compliance
Topic: *Authentication and Password Management*

HIPAA Regulation:

• *Mechanism to authenticate electronic protected health information*	§164.312(c)(1)	addressable
• *Person or entity authentication*	§164.312(d)	required
• *Password management*	§164.308(a)(5)	addressable
• *Unique user identification*	§164.312(a)(1)	required

Purpose:

The purpose of this procedure is to ensure that workforce members select and secure strong passwords to authenticate their access to information systems containing electronic protected health information (EPHI).

Description:

Information systems used to access EPHI shall uniquely identify and authenticate workforce members.

Novell Authentication Standards
The password file on the authenticating server shall be adequately protected and not stored in plaintext (unencrypted).

1. Automatic password expiration at User ID creation and password reset.
2. Automatic password expiration every 90 days.
3. A minimum password length of 8 characters.
4. A minimum of three passwords are retained in the system that cannot be reused with a User ID.

Meditech Authentication Standards
The password file on the authenticating server is stored in an encrypted format.

1. Automatic password expiration at User ID creation and password reset.
2. Automatic password expiration every 30 days.
3. A minimum password length of eight characters, utilizing alphanumeric combination.
4. Passwords will expire after three failed password attempts.

User ID and Password Management

All workforce members are assigned a unique User ID to access the Ulster County network and are responsible for creating and maintaining the confidentiality of the password associated with their unique User ID.

Supervisors and managers are required to ensure that the workforce under their supervision understands the user responsibilities for securely managing confidential passwords.

Upon receipt of a User ID, the workforce member assigned the User ID is required to change the password provided by the administrator to a password that only he or she knows. Strong passwords shall be created in order to secure access to EPHI.

Workforce members who suspect that their password has become known by another person shall immediately request through UCIS customer support to change their password. Work members shall not share with or reveal their password to anyone, including their supervisor, manager, or UCIS IT support staff.

All privileged system-level passwords (e.g., root enable, application administration accounts, etc.) shall be changed, at a minimum, each fiscal quarter.

All passwords are to be treated as sensitive, confidential Ulster County information. If the workforce member's manager or supervisor requires emergency access to a worker's email or individual network drive, refer to **Granting Access in an Emergency** under the ***User Access Management Procedure***.

Strong Password Guidelines

Select strong passwords that have the following characteristics:

1. The password contains at least 8 characters.
2. The password contains both upper and lower case characters.
3. The password contains at least one number or special character (such as @, #, $, %).
4. The password is not so hard to remember that you have to write it down but it should remain difficult for others to guess.
5. Avoid using dictionary words.

Responsibilities:

Manager and Supervisor Responsibilities

1. Reinforce secure password use by workforce members.
2. If access to another workforce member's account is required, follow the emergency access procedures in **Granting Access in an Emergency** under the ***User Access Management Procedure*.**

UCIS IT Support Responsibilities

1. System administrators shall verify the identity and the authority of the workforce member or an authorized requester, such as the member's manager or supervisor, before providing the password for a new User ID.
2. System administrators shall verify the identity and the authority of the workforce member requesting a password reset.
3. System administrators shall verify the identity and the authority of an authorized requester, such as the member's manager or supervisor, to request a password reset for another workforce member.

Workforce Member Responsibilities

1. Create and securely manage strong passwords for access to systems containing EPHI.
2. Follow the password protection requirements to protect the confidentiality of their passwords to ensure security of EPHI:
    - Passwords shall not be shared with or revealed to anyone, including their supervisor, manager, or UCIS IT support staff.
    - Passwords shall never be revealed on questionnaires or security forms.
    - Passwords shall be memorized, not written down.
    - The password used to access Ulster County network shall not be used anywhere else.
    - The password shall be changed immediately if the workforce member suspects it has become known by another person.

Procedure: HIPAA/HITECH Compliance
Topic: *Automatically Forwarded Email*

Purpose:

The purpose of this procedure is to prevent the unauthorized or inadvertent disclosure of sensitive company information.

This procedure covers automatic email forwarding, and thereby the potentially inadvertent transmission of sensitive information by all employees, vendors, and agents operating on behalf of Ulster County.

Description / Responsibilities:

Employees must exercise utmost caution when sending any email from inside Ulster County to an outside network. Unless approved by an employee's manager or UCIS Director/Security Officer, Ulster County email will not be automatically forwarded to an external destination. Sensitive information or any information containing EPHI will not be forwarded via any means, unless that email is critical to business and is encrypted in accordance with the ***Acceptable Encryption Procedure***.

Procedure: HIPAA/HITECH Compliance
Topic: *Breach Notification and Risk Assessment Actions and Response*

HIPAA Regulation:

• *Policy and Procedures*	§164.402-414	required
• *Reporting and response*	§164.308(a)(6)	required

Purpose:

The purpose of this policy is to formalize the response to, and reporting of, Protected Health Information (PHI), Electronic Protected Health Information (EPHI), and Personally Identifiable Information (PII) data security or privacy breach or disclosure incidents. This includes identification and response to suspected or known privacy and security incidents, the mitigation of the harmful effects of known or suspected incidents to the extent possible, and the documentation of incidents and their outcomes.

Description:

Ulster County will respond to all impermissible uses or disclosures of protected health information and it will be presumed that a breach has occurred unless the Ulster County or its business associate, as applicable, demonstrates through the appropriate risk assessment process, that there is a low probability that the protected health information has been compromised. All disclosure, impermissible uses and breach incidents of electronic and hardcopy protected health information shall be reported and responded to promptly.

Workforce Member Responsibilities
Workforce members shall immediately notify their manager or supervisor of any suspected or confirmed breach or disclosure incident. The manager or supervisor shall report the incident to the Compliance Officer, Privacy Officer, and Security Officer at Compliance.Incident@co.ulster.ny.us. The Compliance Officer, Privacy Officer, and Security Officer will, in concert together, evaluate the situation to determine the appropriate response to the report disclosure or breach incident, and initiate the response process as required by the type of incident.

Impermissible Uses, Breach or Disclosures Risk Assessment

The Compliance Officer, Privacy Officer, and Security Officer will WITHOUT UNREASONABLE DELAY:

1. Perform and document a risk assessment based on the disclosure/breach identified: the process to be followed is – based on the current rule:
    a. Instead of assessing the risk of harm to the individual, Ulster County and business associates must assess the probability that the protected health information has been compromised based on a risk assessment that considers at least the following factors:
        i. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification; (remember to include in the review a "sensitivity rating" - For example, with respect to financial information, this includes credit card numbers, social security numbers, or other information that increases the risk of identity theft or financial fraud – and if this is the case, then other laws may come into play);
        ii. The unauthorized person who used the protected health information or to whom the disclosure was made;
        iii. Whether the protected health information was actually acquired or viewed; and
        iv. The extent to which the risk to the protected health information has been mitigated.

Impermissible Uses, Breach or Disclosures Response and Resolution

Ulster County**,** following a breach or suspected breach of unsecured protected health information or PII, shall:

1. Provide notice of a breach to prominent media outlets serving a State or jurisdiction, following the discovery of a breach if the unsecured protected health information of more than 500 residents of such State or jurisdiction is, or is reasonably believed to have been, accessed, acquired, or disclosed during such breach. This notice is in addition, not a substitute to, the required written notice, and shall be provided in the following form:
    a. Written notification by first-class mail to the individual at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification may be provided in one or more mailings as more information becomes available.
    b. If the covered entity knows the individual is deceased and has the address of the next of kin or personal representative of the individual (as specified under §164.502(g)(4) of subpart E) , written notification by first-class mail to either the next of kin or personal representative of the individual. The notification may be provided in one or more mailings as information is available.

c. Substitute notice. In the case where there is insufficient or out-of-date contact information that precludes written notification to the individual, a substitute form of notice reasonably calculated to reach the individual shall be provided. Substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative of the individual.
d. In the case where there is insufficient or out-of-date contact information for fewer than 10 individuals, then substitute notice may be provided by an alternative form of written notice, telephone or other means.
e. In the case in which there is insufficient or out-of-date contact information for 10 or more individuals, then such substitute notice shall: (A) be in the form of either a conspicuous posting for a period of 90 days on the home page of Ulster County's web site, or conspicuous notice in a major print or broadcast media in geographic areas where the individuals affected by the breach likely reside; and (B) include a toll-free number that remains active for at least 90 days where an individual can learn whether the individual's secured protected health information may be included in the breach.
f. In any case deemed by Ulster County to require urgency because of possible imminent misuse of unsecured protected health information, Ulster County may provide information to individuals by telephone or other means, as appropriate, in addition to written notice.
g. Inform prominent media outlets serving the State or jurisdiction.

2. Except as provided in §164.412, Ulster County shall provide the notification required without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.

3. The content of the notification required shall meet the requirements of §164.404(c) and shall include to the extent possible:
    a. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
    b. A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);
    c. Any steps the individual should take to protect themselves from potential harm resulting from the breach;
    d. A brief description of what Ulster County is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches;
    e. Contact procedures for individuals to ask questions or learn additional information which should include a toll-free number, an email address, website, or postal address; and
    f. The notification shall be written in plain language.

Ulster County shall, following the discovery (post risk assessment) of a breach of unsecured protected health information as provided in §164.404(a)(2):

1. Notify the Secretary of HHS.
2. For breaches of unsecured protected health information involving 500 or more individuals, Ulster County will provide the notification required in the manner specified on the HHS web site located at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html.
3. For breaches of unsecured protected health information involving less than 500 individuals, Ulster County shall maintain a log or other documentation of such breaches and, not later than 60 days after the end of each calendar year, provide the notification required for those breaches occurring during the preceding calendar year, in a manner specified on the HHS web site at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html.

Ulster County is required to notify all individuals when there has been or is reasonably believed to have been an unintended disclosure or compromise of the individual's private information (PII, PHR, PHI, etc.) in compliance with the applicable Information Security Breach and Notification Acts affecting Ulster County and this policy.

In addition:

1. Ulster County has in place the appropriate measures to monitor and detect the unauthorized access, disclosure, or compromise to private information stored within our premises or at third parties who store, transmit, or process PHR, PHI, ePHI, and PII on behalf of Ulster County.
2. Ulster County has the ability to assess any third party who stores, processes, or transmits PHI, PHR, or PII on Ulster County's behalf.
3. Ulster County, after consulting with the Information Security Officer to determine the scope of the breach and restoration measures, shall notify the individual when it has been determined that there has been, or is reasonably believed to have been a compromise of private information through unauthorized disclosure.
4. A compromise of private information shall mean the unauthorized acquisition of unencrypted computerized data with private information as identified as PHR, PHI, ePHI, and PII under the applicable laws and regulations.
5. In addition, if encrypted data is compromised along with the corresponding encryption key, the data shall be considered unencrypted and thus fall under the notification requirements.
6. It is understood that notification may be delayed if a law enforcement agency determines that the notification impedes a criminal investigation. In such case, notification will be delayed only as long as needed to determine that notification no longer compromises any investigation.

7. Ulster County shall notify the Compliance Officer, Privacy Officer, and Security Officer as to the timing, content, and distribution of the notices and approximate number of affected persons.
8. Ulster County shall notify the Attorney General, Consumer Protection Boards, and any other required agency or body whenever notification to an affected resident is necessary, as to the timing, breach identifications, content, and distribution of the notices and approximate number of affected persons.
9. Regardless of the method by which notice is provided, such notice shall include contact information for Ulster County making the notification and a description of the categories of information that were, or are reasonably believed to have been, acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, so acquired.
10. This Policy also applies to information maintained on behalf of Ulster County by any third party.
11. When more than five hundred residents are to be notified at one time, Ulster County is required to notify the appropriate consumer reporting agencies, State Agencies, and Federal Agencies as to the timing, content, and distribution of the notices and the approximate number of affected individuals. This notice, however, will be made without delaying notice to the individuals.
12. Ulster County will have in place a **Comprehensive Written Information Security Program (WISP)** that includes at least the following:
    - An effectively designed and operating security program applicable to all records containing personal information (PHR, PHI, ePHI, and PII), both hard copy and electronic.
    - Reasonable administrative, technical, and physical safeguards for PHR, PHI, ePHI and PII protection.
    - Where one or more employees are named to maintain and supervise WISP implementation and performance.
    - Threat assessments performed at least annually and at every significant infrastructure change that measure existing and needed controls and
        - Are based on regulatory and industry standards affecting the data
        - Consider any access to and security of, paper, electronic and other PHR, PHI, ePHI, and PII records, computing systems, and storage media, including laptops and portable devices, wireless, third parties, external partners and any others that contain personal information.
    - Includes annual employee security awareness training and procedures for monitoring employee compliance.
    - Includes disciplinary measures for violators.
    - Includes policies and procedures for all controls regarding when and how records containing PHR, PHI, ePHI, and PII should be kept, accessed, or transported internally and externally.

- Includes processes for immediately blocking terminated employees' physical and electronic access to PHR, PHI, ePHI, and PII records (including deactivating their passwords and user names).
- Reviewing all third-party service provider contracts to confirm they are capable of maintaining appropriate security measures consistent with all the laws and regulations affecting Ulster County.
- Employ the use of experts (internal or external) which asses, implement, and maintain appropriate security measures.
- Will limit to the amount reasonably necessary to accomplish legitimate Ulster County business purposes or to comply with state or federal regulations any PHR, PHI, ePHI, and PII.
- Will limit access to PII to those persons who have an approved "need to know" in connection with legitimate Ulster County business purpose, or in order to comply with state or federal regulations.
- Store paper records and data containing PHR, PHI, ePHI, and PII in locked facilities, storage areas, or containers.
- Implement and test the Incident Response Plan (IRP), for both paper and electronic breach concerns.
- Have in place secure authentication protocols that provide for:
    - Control of user IDs and other identifiers
    - A reasonably secure method of assigning/selecting passwords, or for use of unique identifier technologies (such as biometrics or token devices).
    - Control of data security passwords such that passwords are kept in a location and/or format that does not compromise the security of the data they protect.
    - Restricting access to PII to active users and active user accounts.
    - Blocking access after multiple unsuccessful attempts to gain access.
- Unique identifications plus passwords (which are not vendor supplied default passwords) to each person with computer access; and are those IDs and passwords reasonably designed to maintain the security of those access controls.
- To the extent technically feasible, encrypt all PII records and files that are transmitted across public networks, and that are to be transmitted wirelessly.
- Encrypt all PII stored on laptops or other portable devices such as data storage devices, smartphones, back-up tapes, email, CD/DVD, USB drives, etc.
- Have monitoring in place to alert the Information Security Officer to the occurrence of unauthorized use of or access to PHR, PHI, ePHI, and PII.
- Firewall protection for files containing PHR, PHI, ePHI, and PII.
- Regularly install appropriate operating system and application security patches to maintain the integrity of the PHR, PHI, ePHI, and PII.
- Have up-to-date versions of system security agent software, including malware protection, and up-to-date security patches and virus definitions.

Impermissible Uses, Breach or Disclosures Response and Resolution Logging

Other than the above requirements for reporting to external agencies, all Impermissible Use, Breach, or Disclosure related incidents and their outcomes will be logged by the Compliance Officer, Privacy Officer, and Security Officer and all findings, outcomes, and communications documented. That documentation will be saved for at least seven years or as needed to meet any claims, legal challenges, or other compliance activities.

Each calendar year, the log will be reviewed and disclosures will be reported to the appropriate regulatory agency as required.

Procedure Responsibilities:

1. The Compliance Officer, Privacy Officer, and Security Officer determine if the incident requires further investigation and if it is a breach of PHR, PHI, ePHI, and PII. Working with the affected departments, they shall determine if corrective actions should be implemented.
2. The Compliance Officer, Privacy Officer, and Security Officer are responsible for documentation of PHR, PHI, ePHI, and PII breach investigations and any corrective actions.
3. The Compliance Officer, Privacy Officer, and Security Officer are responsible for maintaining all documentation on PHR, PHI, ePHI, and PII breaches for a minimum of six years.

Procedure: HIPAA/HITECH Compliance
Topic: *Business Associate*

HIPAA Regulation:

- *Business associate contracts and other arrangements* §164.308(b)(1) required
- *Written contract or other arrangements* §164.308(b)(1) required

Purpose:

The purpose of this procedure is to document the process for determining, documenting, and monitoring those contractual and business relationships that are considered "Business Associates" as defined by the HIPAA Security Rule.

Description:

Business Associate Determination

In order to determine if a contractual or business relationship meets the definition of a HIPAA Business Associate as defined by legal mandate, the following process shall be followed:

1. When a contract is developed or a new vendor is added it is the responsibility of the Compliance Officer and Security Officer to ensure that a HIPAA Business Associate Agreement (BAA) is completed, sent to the vendor, returned without unreasonable delay, and reviewed annually or as required.

Business Associate Monitoring

1. If Ulster County knows of a pattern of activity or practice that constitutes a material breach or violation of an obligation of the Business Associate under the contract or other arrangement, Ulster County shall take reasonable steps to repair the breach or end the violation as applicable.
2. Annually or during every required risk assessment, all Business Associates will be assessed on reported on regarding each Business Associates compliance with the BAA and HIPAA rules.

Responsibilities:

Workforce Member Responsibilities

1. Immediately provide information regarding any compliant or report from any source about inappropriate safeguards to PHI by Business Associate contractors to their manager or supervisor.

Manager and Supervisor Responsibilities

1. Respond to any pattern of activity or practice of a HIPAA Business Associate that constitutes a material breach or violation of an obligation of the Business Associate, under the contract or other arrangement, by documenting the incident.
2. Promptly inform and work with Compliance Officer to repair the breach, end the violation, and or terminate the contract, as applicable.

Office of Compliance Responsibilities

1. Maintain a database of all HIPAA Business Associates.
2. Coordinate with Security Officer in responding to a report of any pattern of activity or practice that constitutes a material breach or violation of an obligation of a Business Associate.

Procedure: HIPAA/HITECH Compliance
Topic: *Contingency Plan*

HIPAA Regulation:

• *Contingency plan*	§164.308(a)(7)	required
• *Data backup plan*	§164.308(a)(7)	required
• *Disaster recovery plan*	§164.308(a)(7)	required
• *Emergency mode operation plan*	§164.308(a)(7)	required
• *Testing and revision procedures*	§164.308(a)(7)	addressable
• *Applications and data criticality analysis*	§164.308(a)(7)	addressable
• *Contingency operations*	§164.308(a)(7)	required

Purpose:

The purpose of this procedure is to establish rules to protect the availability, integrity, and security of electronic protected health information (EPHI) while continuing business without the normal resources of the organization.

Description:

Ulster County shall have documented procedures for implementation in the event of an emergency, disaster or other occurrence (i.e., fire, vandalism, system failure, and natural disaster) when any system that contains EPHI is affected, including:

- Applications and Data Criticality Analysis
- Data Backup Plan
- Disaster Recovery Plan
- Emergency Mode Operation Plan

Each of the following plans shall be evaluated and periodically updated as business needs and technology requirements change.

Applications and Data Criticality Analysis

There shall be periodic assessment of the relative criticality of applications and data that contain EPHI for the purposes of maintaining a current Data Backup Plan, Disaster Recovery Plan, and Emergency Mode Operation Plan.

Ulster County shall identify critical business functions, define impact scenarios, and determine resources needed to recover from each impact.

Data Backup Plan

All EPHI shall be stored on network servers in order for it to be automatically backed up by the system.

EPHI shall not be saved on the local (C:) drive of any workstation.

EPHI stored on portable media shall be saved to the network to ensure backup of the EPHI.

UCIS IT support shall establish and implement a Data Backup Plan that, at a minimum, includes daily backups of user-level and system-level information and weekly backups that are stored securely offsite or in the cloud IAW FedRAMP regulations.

The Data Backup Plan shall apply to all files that may contain EPHI.

The Data Backup Plan shall require that all media used for backing up EPHI be stored in a physically secure environment.

Data backup procedures outlined in the Data Backup Plan shall be tested on at least an annual basis to ensure that copies of EPHI can be retrieved and made available.

Disaster Recovery Plan

To ensure that HIPAA covered components can recover from the loss of data due to an emergency or disaster such as fire, vandalism, system failure, or natural disaster affecting systems containing EPHI, IT support shall establish and implement a Disaster Recovery Plan for restoring or recovering loss of EPHI and the systems needed to make that EPHI available in a timely manner.

The Disaster Recovery Plan shall be documented and available to the assigned personnel, who shall be trained to implement the Disaster Recovery Plan.

The disaster recovery procedures outlined in the Disaster Recovery Plan shall be tested on a periodic basis to ensure that EPHI and the systems needed to make EPHI available can be restored or recovered.

Emergency Mode Operation Plan

Ulster County shall document and implement procedures to enable continuation of critical business processes for the protection of EPHI while operating in emergency mode. Emergency mode operation must include processes to protect the security of EPHI during and immediately after a crisis.

Emergency mode operation procedures outlined in the Emergency Mode Operation Plan shall be tested periodically.

Procedure Responsibilities:

Manager and Supervisor Responsibilities

1. Develop and document an Emergency Operations Mode Plan for their units that include appropriate procedures for their workforce.
2. Annually ensure that appropriate emergency operations and disaster recovery procedures are in place.
3. Periodically test their Emergency Operations Mode Plan.
4. Ensure that workforce members save all EPHI on network drives and not on the local drive (C:) of their workstation.

UCIS IT Support Responsibilities

1. Establish, implement, and document the Data Backup Plan for EPHI that is used.
2. Annually test the EPHI backups to ensure that exact copies of EPHI can be retrieved.
3. Document and maintain a Disaster Recovery Plan to restore the EPHI applications and data that is needed for the HIPAA covered components to continue their critical business functions in a disaster.
4. Periodically test the documented disaster recovery procedures to ensure that EPHI data and systems can be restored.

Procedure: HIPAA/HITECH Compliance
Topic: *Device and Media Controls*

HIPAA Regulation:

• *Device and media controls*	§164.310(d)(1)	required
• *Disposal*	§164.310(d)(1)	required
• *Media reuse*	§164.310(d)(1)	required
• *Accountability*	§164.310(d)(1)	required
• *Data backup and storage*	§164.310(d)(1)	required

Purpose:

The purpose of this procedure is to ensure that electronic protected health information (EPHI) stored or transported on storage devices and removable media is appropriately controlled and managed.

Description:

Device and Media Protection
Ulster County shall protect all the hardware and electronic media that contain EPHI. This includes, but is not limited to, workstation computers, laptops, iOS and Android smartphones, USB drives, backup tapes, and CDs/DVDs.

There shall be procedures that govern the receipt and removal of hardware and electronic media that contain EPHI outside of the secured physical perimeter of an Ulster County facility and the movement of these items within the facility. Procedures shall include maintaining a custody record of hardware and electronic media.

Portable Media Security
EPHI that is placed on portable electronic media shall be encrypted so that access to the EPHI can only be attained by authorized individuals with knowledge of the decryption code.

Workforce members shall limit the quantity of EPHI on portable electronic media to the minimum necessary for the performance of their duties.

All workforce members shall receive permission from their supervisor before transporting EPHI outside of the secured physical perimeter of an Ulster County facility. Approvals shall include the time period for authorization, which shall be a maximum of one year.

Workforce members shall not leave portable media that contains EPHI visible in their vehicles or in any other unsecured location.

If portable media is lost, workforce members are responsible to immediately notify their supervisor.

Electronic Media Disposal

Before electronic media that contains EPHI can be disposed, the following actions shall be taken on devices by the workforce:

1. Hard drives shall be either wiped clean by UCIS IT or destroyed to prevent recognition or reconstruction of the information. The hard drive shall be tested to ensure the information cannot be retrieved.
2. County issued mobile devices, smartphones and tablets, shall have all stored EPHI erased or shall be physically destroyed.
3. Storage media such as backup tapes, USB flash drives and CDs, shall be physically destroyed (broken into pieces) before disposing of the item (deliver to UCIS for proper disposition).

Electronic Media Reuse

All EPHI shall be removed from hard drives when the equipment is transferred to a worker who does not require access to the EPHI. Hard drives shall be wiped clean by UCIS IT before transfer.

All other media shall have all the EPHI removed (the mechanism may vary depending on the media type) and tested to ensure the EPHI cannot be retrieved. If the media is not “technology capable” of being cleaned, the media shall be overwritten or destroyed.

Device Maintenance and Repair

When the technology is capable, all EPHI shall be removed from the device’s memory or hard drive before the device is accessed for maintenance or sent out for repair. Devices include computer servers, copiers, printers, and other devices capable of storing electronic data.

Device and Media Acquisition

Ulster County shall include security requirements and/or security specifications in information system acquisition contracts based on an assessment of risk (applications, servers, copiers, etc.).

Responsibilities:

Manager and Supervisor Responsibilities

1. Ensure that only workforce members whose duties require the need to transport EPHI outside of the secured physical perimeter of an Ulster County facility are granted permission to do so.
2. Enforce procedures to govern the receipt and removal of hardware and electronic media that contain EPHI outside of the secured physical perimeter of an Ulster County facility and the movement of these items within the facility.

UCIS IT Support Responsibilities

1. Ensure that all hard drives are wiped clean of EPHI before disposal, reuse, or being sent out for repair.
2. Maintain an inventory and record of movements of hardware and electronic media such as workstation computers, servers, or backup tapes.

Workforce Member Responsibilities

1. Follow the procedures that govern the receipt and removal of hardware and electronic media that contain EPHI.
2. Limit the quantity of EPHI on portable electronic media to the minimum necessary to perform their duties.
3. Secure EPHI on portable electronic media through encryption.
4. Remove and destroy all EPHI from portable electronic media when it is no longer needed to perform their duties.
5. Do not leave or store portable media that contains EPHI in their vehicles or in any other unsecured location.

Procedure: HIPAA/HITECH Compliance
Topic: *Email Use*

Purpose:

The purpose of this procedure is to prevent unauthorized use of County resources and to protect the professional public image of Ulster County. When email is sent from the Ulster County domain, the general public will tend to view that message as an official policy statement from Ulster County.

This procedure covers appropriate use of any email sent from an Ulster County email address and applies to all employees, vendors, and agents operating on behalf of Ulster County.

Description / Responsibilities:

Prohibited Use
The Ulster County email system shall not be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any Ulster County employee should immediately report the matter to their supervisor.

Personal Use
Using a reasonable amount of Ulster County resources for personal emails is acceptable, but non-work related email shall be saved in a separate folder from work related email. Sending chain letters or joke emails from an Ulster County email account is prohibited. Virus or other malware warnings and mass mailings from Ulster County shall be approved by Ulster County Director of Information Services before sending. These restrictions also apply to the forwarding of mail received by an Ulster County employee.

Monitoring
Ulster County employees shall have no expectation of privacy in anything they store, send, or receive on the County's email system. Ulster County may monitor messages without prior notice. Additionally, Ulster County is not obliged to monitor email messages.

Procedure: HIPAA/HITECH Compliance
Topic: *Facility Access Controls*

HIPAA Regulation:

• *Facility security plan*	§164.310(a)(1)	addressable
• *Facility access controls*	§164.310(a)(1)	addressable
• *Access control and validation procedures*	§164.310(a)(1)	addressable
• *Maintenance records*	§164.310(a)(1)	addressable
• *Contingency operations*	§164.310(a)(1)	addressable

Purpose:

The purpose of this procedure is to establish protocols for securing facilities that contain electronic protected health information (EPHI).

Description:

Ulster County shall reasonably safeguard EPHI from any intentional or unintentional use or disclosure. Ulster County shall protect its facilities where EPHI can be accessed.

Facility Security Plan
Ulster County shall safeguard the facilities of its HIPAA covered components and the equipment therein from unauthorized physical access, tampering, and theft.

There shall be periodic audits of HIPAA covered components to ensure EPHI safeguards are continuously being maintained.

When designing a new building and remodeling existing sites, facility managers and/or designees shall work with the Compliance Officer to ensure the facility plan components below are compliant with federal HIPAA regulations.

The following shall be implemented for all sites that access EPHI:

1. **Visitor Access Control**: In facilities in which EPHI is available, all visitors shall be escorted and monitored. Each facility shall implement procedures that govern visitor access controls. These procedures may vary depending on the facility structure, the type of visitors, and where the EPHI is accessible.

2. **Keypads/Cipher Locks**: Facilities shall change the codes on keypads/cipher locks at least every six months in order to ensure the security of staff and property and the confidentiality of client information. In addition, the facility shall have:
    a) Clearances based on programmatic need, special mandated security requirements, and workforce member security; and
    b) A mechanism to track which workforce members are provided access.
3. **Metal/Hard Keys**: Facilities that use metal/hard keys shall change affected or appropriate key locks when keys are lost or a workforce member leaves without returning the key. In addition, the facility shall have:
    a) Clearances based on programmatic need, special mandated security requirements, and workforce member security; and
    b) A mechanism to track which workforce members are provided access.
4. **Network Closet(s):** Every network closet shall be locked, whenever the closet is unoccupied or not in use, or shall be enclosed in a locked equipment cage. HIPAA covered components shall maintain a log of who has accessed the network closets and periodically change the locking mechanism to these closets.
5. **Server Room(s):** Every server room shall be locked whenever the room is unoccupied or not in use, or shall be enclosed in a locked equipment cage. HIPAA covered components shall document who has access to each server room and periodically change the locking mechanism to server rooms.
6. **Alarm Systems:** All buildings that contain EPHI shall have some form of alarm system that is activated during non-business hours. Alarm system codes may only be provided to workforce members who require this information in order to leave and enter a building.
7. **Doors:** All non-public exterior doors (such as employee only doors) and doors leading to areas with EPHI shall remain locked at all times. It is each workforce member's responsibility to make sure the door that is being entered or exited is completely shut before leaving the door. If a door's closing or locking mechanism is not working, it is every worker's responsibility to notify the facility manager or designee for that facility.

Contingency Operations – Emergency Access to Facilities

Each facility shall have emergency access procedures in place that allow facility access for appropriate workforce members to access EPHI as well as support restoration of lost EPHI. This includes a primary contact person and back-up person when facility access is necessary after business hours by persons who do not currently have access to the facility outside of regular business hours.

Maintenance Records

Repairs or modifications to the physical building for each facility where EPHI can be accessed shall be logged and tracked. The log shall include, at a minimum, events that are related to security (for example, repairs or modifications of hardware, walls, doors, and locks).

Procedure Responsibilities:

Supervisor and Manager Responsibilities

1. Take appropriate corrective action if any workforce member knowingly violates the facility security plan and its procedures.
2. Authorize clearances that are appropriate to the duties of each workforce member.
3. Notify the manager or designee within one business day when a user no longer requires access to the facility.
4. Verify that each workforce member surrenders her/his card or key upon leaving employment.
5. Work with facility manager to ensure a log is kept of all access into network closets.

Workforce Member Responsibilities

1. Display their access/security card or employee badge to demonstrate their authorization to access restricted areas.
2. Do not allow other persons to enter the facility by “tailgating” (entering the facility by walking behind an authorized person through a door without valid identification).
3. Do not share access hard keys, alarm codes or keypad codes to enter the facility or areas where there is EPHI.
4. Immediately report lost or stolen ID cards, metal keys, or keypad-cipher lock combinations.
5. Surrender ID cards and/or hard key(s) upon leaving employment.

Facility Manager Responsibilities

1. Request and track maintenance repairs.
2. Establish and maintain a mechanism for accessing the facility in an emergency.
3. Track who has access to the facility.
4. Change metal locks when a key is lost or unaccounted for.
5. Change combination keypads/cipher locks every three months.

Corporate Compliance and HIPAA Compliance Officer Responsibilities

1. Work with managers to ensure that all Ulster County facilities comply with the HIPAA Security Rule for access controls.
2. Conduct periodic audits of HIPAA covered components to ensure their facilities are secure and the requirements of this policy are enforced.

Procedure: HIPAA/HITECH Compliance
Topic: *Internet DMZ Equipment*

Purpose:

The purpose of this procedure is to define standards to be met by all equipment owned and/or operated by Ulster County located outside the County's Internet firewalls. These standards are designed to minimize the potential exposure to Ulster County from the loss of sensitive or company confidential data, intellectual property, damage to public image, etc. that may follow from unauthorized use of Ulster County resources.

Devices that are Internet facing and outside the Ulster County firewall are considered part of the "demilitarized zone" (DMZ) and are subject to this policy. These devices (network and host) are particularly vulnerable to attack from the Internet since they reside outside the County firewalls.

The procedure defines the following standards:

- Ownership responsibility
- Secure configuration requirements
- Operational requirements
- Change control requirement

All equipment or devices deployed in a DMZ owned and/or operated by Ulster County (including hosts, routers, switches, etc.) and/or registered in any Domain Name System (DNS) domain owned by Ulster County must follow this policy.

This procedure also covers any host device outsourced or hosted at external/third-party service providers, if that equipment resides in the "UlsterCountyNY.gov" domain or appears to be owned by Ulster County.

All new equipment that falls under the scope of this procedure must be configured according to the referenced configuration documents, unless a waiver is obtained from UCIS. All existing and future equipment deployed on Ulster County's un-trusted networks must comply with this policy.

Procedure Description / Responsibilities:

Ownership and Responsibilities
Equipment and applications within the scope of this procedure must be administered by support groups approved by UCIS for DMZ system, application, and/or network management.

Support groups will be responsible for the following:

- Equipment must be documented in the County-wide enterprise management system. At a minimum, the following information is required:
    - Host contacts and location.
    - Hardware and operating system/version.
    - Main functions and applications.
    - Password groups for privileged passwords.
- Network interfaces must have appropriate Domain Name Server records (minimum of A and PTR records).
- Password groups must be maintained in accordance with the County-wide password management system/process.
- Immediate access to equipment and system logs must be granted to authorized members of UCIS upon demand.
- Changes to existing equipment and deployment of new equipment must follow any corporate governance or change management processes/procedures.

To verify compliance with this policy, UCIS will periodically audit DMZ equipment.

General Configuration Procedure

All equipment must comply with the following configuration(s):

- Hardware, operating systems, services, and applications must be approved UCIS as part of the pre-deployment review phase.
- Operating system configuration must be done according to the secure host and router installation and configuration standards.
- All patches/hot-fixes recommended by the equipment vendor and UCIS must be installed. This applies to all services installed, even though those services may be temporarily or permanently disabled. Administrative owner groups must have processes in place to stay current on appropriate patches/hot fixes.
- Services and applications not serving business requirements must be disabled.
- Trust relationships between systems may only be introduced according to business requirements, must be documented, and must be approved by UCIS.
- Services and applications not for general access must be restricted by access control lists.
- Insecure services or protocols (as determined by UCIS) must be replaced with more secure equivalents whenever such exist.
- Remote administration must be performed over secure channels (e.g., encrypted network connections using SSH or IPSEC) or console access independent from the DMZ networks. Where a methodology for secure channel connections is not available, one- time passwords (DES/SofToken) must be used for all access levels.
- All host content updates must occur over secure channels.

- Security-related events must be logged and audit trails saved to UCIS approved logs. Security related events include (but are not limited to) the following:
    - User login failures.
    - Failure to obtain privileged access.
    - Access policy violations.
- UCIS will address non-compliance waiver requests on a case-by-case basis and approve waivers if justified.

New Installations and Change Management Procedures

All new installations and changes to the configuration of existing equipment and applications must adhere to the following policies/procedures:

- Configuration changes must follow the Corporate Change Management (CM) Procedures.
- UCIS must be invited to perform system/application audits prior to the deployment of new services.
- UCIS must be engaged, either directly or via CM, to approve all new deployments and configuration changes.

Equipment Outsourced to External Service Providers

The responsibility for the security of the equipment deployed by external service providers must be clarified in the contract with the service provider and security contacts, and escalation procedures documented. Contracting departments are responsible for third party compliance with this procedure.

Note: External service providers found to have violated this procedure may be subject to financial penalties, up to and including termination of contract.

Procedure: HIPAA/HITECH Compliance
Topic: *Mobile Devices*

Purpose:

Ulster County has a requirement to protect its information technology assets to safeguard its citizens, workforce, customers, intellectual property, and reputation. This document outlines a set of practices and requirements for the safe use of mobile devices.

1. All mobile devices are in scope of this procedure, whether owned by Ulster County or owned by employees, that have access to County networks, data, and systems, not including UCIS managed laptops. This includes all smartphones and tablet computers.
2. Exemptions are only allowed when approved by management in writing and where a risk assessment has been conducted and reported to management.

Procedure Description / Responsibilities:

Technical Requirements

1. Devices must use the latest available Android or iOS Operating Systems.
2. Devices must store all user-saved passwords in an encrypted password store.
3. Devices must be configured with a secure password that complies with Ulster County's password policy (6-digit PIN). This password must not be the same as any other credentials used within the organization.
4. Devices must have installed and properly functioning remote-wipe capable software.
5. Except for those devices managed by UCIS, devices are not allowed to be connected directly to the internal County network.

User Requirements

1. Users must only load data essential to their role onto their mobile device(s).
2. Users must immediately report all missing, lost, stolen, or damaged (MLSD) devices to their immediate supervisor and UCIS.
3. If a user suspects that unauthorized access to County data has taken place via a mobile device the user must report the incident in accordance with Ulster County's incident handling process.
4. Devices must not be "jailbroken" or have any software/firmware installed that is designed to gain access to functionality not intended to be exposed to the user.
5. Users must not load pirated software or illegal content onto their devices.
6. Applications must only be installed from official platform-owner approved sources. Installation of code from un-trusted sources is forbidden. If you are unsure if an application is from an approved source, contact UCIS Customer Support at customersupport@co.ulster.ny.us or (845) 334-5381.

7. Devices must be kept up to date with manufacturer or network provided patches. At a minimum, patches should be checked for weekly and applied at least once a month.
8. Devices must not be connected to a PC that does not have up-to-date and enabled anti-malware protection and which does not comply with County policy.
9. Devices must be encrypted in line with Ulster County's compliance standards.
10. Users must be cautious about the merging of personal and work email accounts on their devices. End-users must take care to ensure that County data is only sent through the County email system. If a user suspects that County data has been sent from a personal email account, either in body text or as an attachment, he or she should immediately notify their supervisor, or next person in their leadership chain (if suspected email derived from supervisor) and UCIS.
11. Unless it is part of the employee's official duties, photographs taken with mobile phones are prohibited within Ulster County buildings and grounds.

Procedure: HIPAA/HITECH Compliance
Topic: *Procedure Documentation*

HIPAA Regulation:

• *Policies and procedures*	§164.316(a)	required
• *Documentation*	§164.316(b)(1)	required
• *Time limit*	§164.316(b)(1)	required
• *Availability*	§164.316(b)(1)	required
• *Updates*	§164.316(b)(1)	required

Purpose:

The purpose of this policy is to establish the process by which Ulster County HIPAA Security Rule Policies and Procedures are created and maintained in accordance with federal regulations.

Description:

Ulster County is required to have policies and procedures for compliance with the HIPAA Security Rule. All policies will be updated annually or at any significant infrastructure change.

Policies and Procedures

1. New or revised HIPAA Security Rule Policies and Procedures as required due to:
    a. Changes in business practices or the Information Technology (IT) environment of the HIPAA covered components
    b. Mandated federal law enacted by Congress
    c. Risk analysis determines new or increased vulnerability to security threat
2. All policies and procedures implemented to comply with the HIPAA Security rule shall be made available to the HIPAA covered component workforce.
3. All actions, activities, or assessments required by the HIPAA Security Policies and Procedures shall be documented. The documentation shall provide sufficient detail to communicate the implemented security measures and to facilitate periodic evaluations by the HIPAA covered components or as requested by the Security Officer.
4. In accordance with 45 C.F.R. § 164.316, documentation shall be retained for a minimum of six (6) years from the time of its creation or the date it was last in effect, whichever is later.

Procedure Responsibilities:

Compliance Responsibilities

1. Draft new or updated HIPAA Security Rule Policies and Procedures as indicated in the **Policies and Procedures** section above.
2. Communicate the approved new or revised policy to the workforce of the HIPAA covered components, and update training and related materials as needed.
3. Maintain and make available to the workforce the HIPAA Security Rule Policies and Procedures in electronic form.

Director, Information Services / Security Officer Responsibilities

Provide final approval of the Ulster County HIPAA Security Policies and Procedures.

Procedure: HIPAA/HITECH Compliance
Topic: *Protection from Malicious Software*

HIPAA Regulation:

- *Protection from malicious software* §164.308(a)(5) addressable

Purpose:

The purpose of this procedure is to establish criteria for protections to guard against, detect, and report malicious software. Malicious software includes, but is not limited to, viruses, worms, malware, ransomware, and spyware.

Description:

Ulster County shall ensure that all workstations install and maintain current anti-virus software. All workstations shall be configured to activate and update anti-virus software automatically whenever the computer is turned on and connected to the network.

In the event that a virus or other malicious code has infected or been identified on a server or workstation that poses a significant risk, that equipment shall be disconnected from the network until it has been appropriately sanitized.

Policy Responsibilities:

Workforce Member Responsibilities

1. Disabling automatic virus scanning features is prohibited.
2. Maintain current anti-virus software on their non-Ulster County computer if it is used to access EPHI.
3. Immediately contact the manager or supervisor and UCIS Customer Support if a virus is suspected, as explained in the ***Security Incident Reporting, Risk Assessment, and Response Procedure***.

UCIS IT Support Responsibilities

1. Maintain current anti-virus software on all HIPAA covered component workstations.
2. Configure laptops to activate and update anti-virus software automatically whenever the computer is turned on and connected to the network.
3. Inform supervisors/department heads/management of any new virus or other malware that may be a threat to EPHI.
4. Disconnect any server or workstation from the network until it has been appropriately sanitized if infected by a virus, worm, or other malicious code that poses a threat to EPHI.

Manager and Supervisor Responsibilities

1. Ensure that laptops used to logon to the network shall have all anti-virus software updates installed by UCIS IT support.
2. Ensure workforce members are made aware of the threats and vulnerabilities due to viruses and malware.
3. Inform workforce members of any new virus, worm, or other type of malicious code that may be a threat to EPHI.

Anti-Virus Process Guidelines

Recommended processes to prevent virus problems are as follows:

- Always run the County standard; supported anti-virus software is available from and managed by UCIS.
- NEVER open any files or macros attached to an email from an unknown, suspicious, or untrustworthy source. Delete these attachments immediately, then “double delete” them by emptying your Trash bin.
- Delete spam, chain, and other junk email without forwarding, in accordance with Ulster County’s ***Acceptable Use Policy***.
- Never download files from unknown or suspicious sources.
- Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so.
- Always scan a USB memory device from an unknown or known source for viruses before attempting to use it.
- Back-up critical data and system configurations on a regular basis and store the data in a safe place.

Procedure: HIPAA/HITECH Compliance
Topic: *Remote Access*

Purpose:

The purpose of this procedure is to define standards for connecting to Ulster County's network from any host. These standards are designed to minimize the potential exposure to Ulster County from damages that may result from unauthorized use of Ulster County resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical Ulster County internal systems, etc.

This procedure applies to all Ulster County employees, contractors, vendors, and agents with an Ulster County owned or personally owned computer or workstation used to connect to the Ulster County network. This policy applies to remote access connections used to do work on behalf of Ulster County, including reading or sending email and viewing intranet web resources.

Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, ISDN, DSL, VPN, SSH, and cable modems, etc.

Procedure Description / Responsibilities:

General

1. It is the responsibility of Ulster County employees, contractors, vendors, and agents with remote access privileges to Ulster County's network to ensure that their remote access connection is given the same consideration as the user's on-site connection to Ulster County resources.
2. No personal use of Ulster County equipment is permitted.
3. Please review the following policies for details of protecting information when accessing the corporate network via remote access methods, and acceptable use of Ulster County's network:
    a. ***Acceptable Encryption Policy*.**
    b. ***Virtual Private Network (VPN) Policy*.**
    c. ***Wireless Communications Policy*.**
    d. ***Acceptable Use Policy*.**

Requirements

1. Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong pass-phrases. For information on creating a strong pass-phrase, see the ***Authentication and Password Management Policy***.
2. At no time should any Ulster County employee provide their login or email password to anyone, including family members.

3. Ulster County employees and contractors with remote access privileges must ensure that their Ulster County owned or personal computer or workstation, which is remotely connected to Ulster County's network, is not connected to any other network at the same time, except for personal networks that are under the complete control of the user.
4. Ulster County employees and contractors with remote access privileges to Ulster County's network must not use non- Ulster County email accounts (i.e., Gmail, Hotmail, Yahoo), or other external resources to conduct Ulster County business, thereby ensuring that official business is never confused with personal business.
5. Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.
6. Non-standard hardware configurations must be approved by UCIS.
7. All hosts that are connected to Ulster County internal networks via remote access technologies must use the most up-to-date anti-virus software, this includes personal computers.
8. Personal equipment that is used to connect to Ulster County's networks must meet the requirements of Ulster County-owned equipment for remote access.
9. Organizations or individuals who wish to implement non-standard remote access solutions to the Ulster County production network must obtain prior approval UCIS.

Procedure: HIPAA/HITECH Compliance
Topic: *Risk Analysis and Management*

HIPAA Regulation:

• *Perform a periodic technical and non-technical evaluation*	§164.308(a)(8)	required
• *Security management process*	§164.308(a)(1)	required
• *Risk analysis*	§164.308(a)(1)	required
• *Risk management*	§164.308(a)(1)	required
• *Information System Activity Review*	§164.308(a)(1)	required

Purpose:

The purpose of this procedure is to establish periodic evaluations of potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (EPHI) held by Ulster County and to manage the security of the EPHI by identifying, controlling, and mitigating risks.

Description:

Ulster County shall perform risk analysis and management through periodic assessments and implementation of controls to mitigate risks.

Risk Analysis
In order to conduct an accurate and thorough assessment of potential risks and vulnerabilities to the EPHI held by Ulster County, the following activities shall be conducted and documented:

1. Periodic program assessments including a security review of facility access controls, protection of network server closets, workstations, portable devices, and document destruction capabilities.
2. Assessments of new or existing information system applications that contain, or are used to protect EPHI.
3. Assessments of modifications to existing facilities or development of new facilities that maintain or house EPHI.
4. Assessments of new programs, departments, or changes in the mode or manner of service delivery involving EPHI.

Risk Management

Security measures and controls, sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level, shall be implemented:

1. Workforce security training and awareness reminders
2. Access controls, authorization and validation procedures
3. Detection and activity reviews
4. Applications and data criticality analysis
5. IT systems change management
6. Incident reporting and response procedures
7. Sanctions for non-compliance
8. Contingency, Data Backup, and Disaster Recovery Planning

IT Change Management

The risk management process shall include change controls for all alterations that occur in the information systems that support, contain, or protect EPHI. These alterations include but are not limited to:

1. Installation, update, or removal of network services and components
2. Operating systems upgrades
3. Installation, update, or removal of applications, software, and database servers

IT change management notification and implementation shall follow the policies and procedures as documented by UCIS IT support.

Procedure Responsibilities:

UCIS IT Support Responsibilities

1. Inform the Office of Compliance of the planned installation, update, or removal of any applications containing EPHI in a HIPAA covered component.

Procedure: HIPAA/HITECH Compliance
Topic: *Router Security*

Purpose:

This document describes a required minimal security configuration for all routers and switches connecting to a production network or used in a production capacity at or on behalf of Ulster County.

All routers and switches connected to Ulster County production networks are affected. Routers and switches within internal, secured labs are not affected. Routers and switches within DMZ areas fall under the ***Internet DMZ Equipment Policy***.

Description / Responsibilities:

Every router must meet the following configuration standards:

1. The enable password on the router must be kept in a secure encrypted form. The router must have the enable password set to the current production router password from the router's support organization.
2. Disallow the following:
    a. IP directed broadcasts
    b. Incoming packets at the router sourced with invalid addresses such as RFC1918 address
    c. TCP small services
    d. UDP small services
    e. All source routing
    f. All web services running on router
3. Use County standardized SNMP community strings.
4. Access rules are to be added as business needs arise.
5. The router must be included in the Ulster County enterprise management system with a designated point of contact.
6. Each router must have the following statement posted in clear view:
   "UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. You must have explicit permission to access or configure this device. All activities performed on this device may be logged, and violations of this policy may result in disciplinary action, and may be reported to law enforcement. There is no right to privacy on this device."

Procedure: HIPAA/HITECH Compliance
Topic: *Sanctions*

HIPAA Regulation:

- *Sanction policy* §165.308(a)(1) required

Purpose:

The purpose of this procedure is to ensure that workforce members of Ulster County are informed of sanctions, penalties, and disciplinary actions that may be applied for non- compliance with Ulster County HIPAA Security Policies and Procedures.

Description:

Workforce members are accountable for their actions in failing to comply with HIPAA Security Rule requirements, as defined in the Ulster County HIPAA Security Policies and Procedures.

Sanctions
Members of the Ulster County workforce who violate HIPAA Security Policies and Procedures regarding the safeguarding of electronic protected health information (EPHI) are subject to disciplinary action by Ulster County up to and including immediate dismissal from employment or service. For violations of these policies by non-employees, corrective action includes but is not limited to contract cancellation or termination of services.

Members of the Ulster County workforce who knowingly and willfully violate state or federal law for failure to safeguard EPHI are subject to criminal investigation, prosecution, and/or civil monetary penalties.

If Ulster County fails to enforce security safeguards, it may be subject to administrative penalties by the federal Department of Health and Human Services Office for Civil Rights, including federal funding penalties.

Reporting Violations
All workforce members shall notify their manager or supervisor, the Compliance Officer, or Security Officer, or Privacy Officer when there is a reasonable belief that any security policies or procedures are being violated.

Retaliation Prohibited

Neither Ulster County as an entity nor any member of Ulster County covered workforce shall intimidate, threaten, coerce, discriminate against, or take any other form of retaliatory action against any individual for:

1. Exercising any right established under the Ulster County HIPAA Security Policies and Procedures
2. Participating in any process established by Ulster County HIPAA Security policy including the filing of a complaint with the Ulster County or with the federal Department of Health and Human Services Office for Civil Rights
3. Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing relating to the policies and procedures

Any workforce member who engages in retaliation shall be subject to the sanctions under this policy.

Procedure Responsibilities:

Workforce Member Responsibilities

1. All HIPAA covered workforce members shall comply with the Ulster County HIPAA Security Policies and Procedures.
2. All HIPAA covered workforce members shall notify their manager or supervisor, the Compliance Officer, or the Security Officer if they have a reasonable belief that any security policies or procedures are being violated.
3. All HIPAA covered workforce members are required to sign HIPAA Acknowledgement Form, certifying they have received training on the Ulster County HIPAA Privacy and Security Policies and Procedures, and will comply with the HIPAA Privacy and Security Policies and Procedures.

Procedure: HIPAA/HITECH Compliance
Topic: *Security Awareness and Training*

HIPAA Regulation:

• *Security awareness and training*	§164.308(a)(5)	addressable
• *Security reminders*	§164.308(a)(5)	addressable

Purpose:

The purpose of this policy if to ensure the workforce receives the necessary training to comply with Ulster County HIPAA Security Policies and Procedures and prevent any violations of confidentiality, integrity, or availability of electronic protected health information (EPHI).

Description:

Workforce training is required to protect EPHI held by Ulster County.

Training Standards

Systems and Applications

Ulster County shall train the workforce, at a minimum, on the following security standards for all systems and applications where access has been granted:

1. Proper uses and disclosures of the EPHI stored in the application
2. How to properly logon and log off the application containing EPHI.
3. Instructions on contacting a manager or supervisor or UCIS Customer Service when EPHI may have been altered or destroyed due to user error.
4. Instructions on reporting a potential security breach to a supervisor, manager, or directly to the UCIS Customer Support.
5. Instructions regarding internet security, virus protection, password security, and confidential data handling.

HIPAA Security Policies and Procedures

The Compliance Officer will provide HIPAA security training to all workforce members on Ulster County's HIPAA Security Policies and Procedures and shall maintain training records for a period of at least six years.

The training will be specific to the roles and responsibilities of the workforce at the worker level and the manager or supervisor level.

All new workforce members in HIPAA covered components are required to attend the appropriate training within 60 days of assuming their position. Workforce members shall attend retraining at a minimum of every three years.

HIPAA Security Reminders

Ulster County shall develop and issue periodic reminders on security awareness to the covered workforce using any media that is most effective (e.g. email, posters, newsletters, intranet site, etc.).

Procedure Responsibilities:

Manager and Supervisor Responsibilities

1. Ensure that all HIPAA workforce members in their operational areas are trained on the systems and application security listed in the **Systems and Applications Training Standards** section above.
2. Ensure all workforce members in their operational areas are enrolled in one of the training classes provided by the Compliance Officer within 60 days of the workforce member assuming their position in the HIPAA covered component.

Workforce Member Responsibilities

1. Workforce members shall complete HIPAA training within 60 days of assuming their position and thereafter once every three years; shall sign the HIPAA Privacy and Security Practices Acknowledgment Form, and provide the signed form to their supervisor or to the Compliance Officer.
2. Temporary agency workforce members, volunteers, and contracted workers that access EPHI are required to provide the Compliance Officer a signed copy of the HIPAA Privacy and Security Practices.

Compliance Officer Responsibilities

1. The Compliance Officer has oversight responsibility to audit reports to ensure required workforce member attendance.
2. The Compliance Officer or its designee shall provide HIPAA security training, track completion of the training and maintain training records for a minimum of six years.
3. The Compliance Officer shall provide periodic security reminders to HIPAA covered component workforce.

Procedure: HIPAA/HITECH Compliance
Topic: *Security Incident Reporting, Risk Assessment, and Response*

HIPAA Regulation:

• *Security incident procedures*	§164.308(a)(6)	required
• *Reporting and response*	§164.308(a)(6)	required

Purpose:

The purpose of this procedure is to formalize the response to, and reporting of, security incidents. This includes identification and response to suspected or known security incidents, the mitigation of the harmful effects of known or suspected security incidents to the extent possible, and the documentation of security incidents and their outcomes.

Description:

Ulster County shall identify, document, and respond to unauthorized use of the systems that contain electronic protected health information (EPHI).

Incident Reporting
All security incidents, threats to, or violations of, the confidentiality, integrity, or availability of electronic protected health information (EPHI) shall be reported and responded to promptly.

Incidents that shall be reported include, but are not limited to:

1. EPHI data loss due to disaster, failure, error, or theft
2. Loss of any electronic media that contains EPHI
3. Loss of the integrity of EPHI
4. Virus, malware, or other malicious cyber attacks
5. Persistent network or system intrusion attempts from a particular entity
6. Unauthorized access to EPHI, or an EPHI-based system or network
7. Facility incidents, including but not limited to:
    - Unauthorized person found in a HIPAA covered component's facility
    - Facility break-in
    - Lost or stolen key, badge, or cardkey

Workforce members shall notify their manager or supervisor of any suspected or confirmed security incident. The manager or supervisor shall report the incident to UCIS Customer Support at (845) 334-5381. UCIS Customer Support will evaluate the situation to determine if it is a potential security threat and initiate the response process as required by the type of incident.

If a facility incident occurs, the manager or supervisor shall immediately report the incident to their facility manager, and to UCIS Customer Support if appropriate.

If the security involves any breach of EPHI, the manager or supervisor shall notify the Compliance Officer and Security Officer, in addition to notifying UCIS Customer Support.

Incident Response and Resolution
UCIS Customer Support shall receive and record basic information on the incident and forward the information to the appropriate staff for response to the type of incident, i.e., a computer virus incident to the UCIS staff that provides anti-virus support.

Subsequently, the UCIS staff receiving the security incident service request shall perform their assigned responsibilities to respond to and/or mitigate any incident consequences. The UCIS staff responsible for determining if a possible EPHI breach has resulted from the incident shall notify both the Compliance Officer and Security Officer.

The Compliance Officer and Security Officer shall evaluate the incident to determine if a breach of EPHI occurred. If it is determined that a breach has occurred, the Compliance Officer and Security Officer shall perform and document risk assessments on such breaches. The Compliance Officer and Security Officer shall then coordinate any mandated notification processes.

Incident Logging
All HIPAA security related incidents and their outcomes will be logged by the UCIS Customer Support and documented by the assigned UCIS support staff. The Compliance Officer and Security Officer shall document and log incidents and outcomes that are reviewed and investigated by that office.

Each fiscal quarter, the assigned UCIS support staff shall provide the Compliance Officer and Security Officer with a record of all the incidents logged. The Compliance Officer and Security Officer will retain these incident reports for six years.

Procedure Responsibilities:

Workforce Member Responsibilities
Workforce members are responsible to promptly report any potential security related incident to their manager or supervisor, and directly to UCIS Customer Support at (845) 334-5381 or customersupport@co.ulster.ny.us.

Supervisor and Manager Responsibilities

1. Ensure UCIS Customer Support, Compliance Officer and Security Officer are notified of any security incident.
2. Ensure the facility manager is notified of any facility related incident as described in the **Incident Reporting** section above.

Manager/Supervisor Responsibilities

Ensure that facility-related security incidents are reported and responded to as directed by the HIPAA covered component's policies and procedures.

UCIS Customer Support Responsibilities

1. Log all reported security incidents for HIPAA covered components.
2. Perform duties to investigate, respond to, and/or mitigate any incident consequences.
3. Notify Compliance Officer and Security Officer when a breach of EPHI is suspected or may have occurred.
4. Provide a report to Compliance Officer and Security Officer quarterly, to be retained for six years.

Compliance Officer and Security Officer Responsibilities

1. Determine if the incident requires further investigation and if it is a breach of EPHI. Working with the affected departments, determine if corrective actions should be implemented.
2. Document EPHI breach investigations and any corrective actions.
3. Maintain all documentation on EPHI breaches for a minimum of six years.

Procedure: HIPAA/HITECH Compliance
Topic: *Server Security*

Purpose:

The purpose of this procedure is to establish standards for the base configuration of internal server equipment that is owned and/or operated by Ulster County. Effective implementation of this policy will minimize unauthorized access to Ulster County proprietary information and technology.

This procedure applies to server equipment owned and/or operated by Ulster County, and to servers registered under any County-owned internal network domain.

This policy is specifically for equipment on the internal Ulster County network. For secure configuration of equipment external to Ulster County on the DMZ, refer to the ***Internet DMZ Equipment Policy***.

Procedure Description / Responsibilities:

Ownership and Responsibilities

All internal servers deployed at Ulster County must be owned by an operational group that is responsible for system administration. Approved server configuration guides must be established and maintained by each operational group, based on business needs and approved by UCIS. Operational groups should monitor configuration compliance and implement an exception policy tailored to the environment. Each operational group must establish a process for changing the configuration guides, which includes review and approval by UCIS.

- Servers must be registered within the County enterprise management system. At a minimum, the following information is required to positively identify the point of contact:
  - Server contact(s) and location, and a backup contact
  - Hardware and Operating System/Version
  - Main functions and applications, if applicable
- Information in the County enterprise management system must be kept up-to-date.
- Configuration changes for production servers must follow the appropriate change management procedures.

General Configuration Guidelines

- Operating System configuration should be in accordance with approved IT guidelines.
- Services and applications that will not be used must be disabled where practical.
- Access to services should be logged and/or protected through access-control methods such as TCP Wrappers, if possible.

- The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.
- Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication will do.
- Always use standard security principles of least required access to perform a function.
- Do not use root when a non-privileged account will do.
- If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).
- Servers should be physically located in an access-controlled environment.
- Servers are specifically prohibited from operating from uncontrolled cubicle areas.

Monitoring

- All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:
  - All security related logs will be kept online for a minimum of one week.
  - Daily incremental tape backups will be retained for at least one month.
  - Weekly full tape backups of logs will be retained for at least one month.
  - Monthly full backups will be retained for a minimum of two years.
- Security-related events will be reported to UCIS management, who will review logs and report incidents to Information Systems management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
  - Port-scan attacks.
  - Evidence of unauthorized access to privileged accounts.
  - Anomalous occurrences that are not related to specific applications on the host.

Compliance

- Audits will be performed on a regular basis by authorized organizations within Ulster County.
- Audits will be managed by the internal audit group and/or UCIS. UCIS will filter findings not related to a specific operational group and then present the findings to the appropriate support staff for remediation or justification.
- Every effort will be made to prevent audits from causing operational failures or disruptions.

Procedure: HIPAA/HITECH Compliance
Topic: *Software Installation*

Purpose:

The purpose of this procedure is to minimize the risk of loss of program functionality, the exposure of sensitive information contained within Ulster County computing network, the risk of introducing malware, and the legal exposure of running unlicensed software.

This procedure covers all IT assets to include, servers, mobile devices/ smartphones, or other devices operating within or connecting to the Ulster County network.

Procedure Description / Responsibilities:

Employees may not install software on Ulster County computing devices operated within the County network. Software requests must first be approved by the requester's manager and then be made to UCIS in writing via the County's IT ticketing request system found on the County's intranet portal. Software must be selected from an approved software list maintained by the UCIS. However, if the County does not possess licensing for a required software, UCIS may obtain and track the licenses, test new software for conflict and compatibility, and perform the installation once properly vetted and funded.

Procedure: HIPAA/HITECH Compliance
Topic: *Transmission Security*

HIPAA Regulation:

• *Transmission security*	§164.312(e)(1)	addressable
• *Integrity controls*	§164.312(e)(1)	addressable
• *Encryption*	§164.312(e)(1)	addressable

Purpose:

The purpose of this procedure is to guard against unauthorized access to, or modification of, electronic protected health information (EPHI) that is being transmitted over an electronic communications network. When EPHI is transmitted from one point to another, it shall be protected in a manner commensurate with the associated risk.

Description:

Encryption

Proven, standard algorithms shall be used as the basis for encryption technologies. The use of proprietary encryption algorithms is not allowed for any purpose.

Encryption Required

1. No EPHI shall be sent outside the Ulster County Wide Area Network (WAN) unless it is encrypted. This includes all email and email attachments sent over the Internet.
2. When accessing a secure network an encryption communication method, such as a Virtual Private Network (VPN), shall be used.

Encryption Optional

1. When using a private circuit (point to point) to transmit EPHI, such as authorized transmission of EPHI within the Ulster County WAN, no encryption is required.

EPHI Transmissions Using Wireless LANs

1. The transmission of EPHI over a wireless network is permitted if both of the following conditions are met:
   a) The connection through the wireless network utilizes an authentication mechanism to ensure that wireless devices connecting to the network are authorized

   b) The connection through the wireless network utilizes an encryption mechanism for all transmissions over the network
2. If transmitting EPHI over a wireless network that is not utilizing an authentication and encryption mechanism, the EPHI shall be encrypted before transmission.
3. Wireless devices are not to be connected to a wireless access point and to the Ulster County WAN at the same time. Wireless access capability must be disabled on any device that is connected to the Ulster County WAN.

Perimeter Security

1. Any external connection to the Ulster County WAN shall come through the perimeter security's managed point of entry.
2. If determined safe, outbound services shall be initiated for internal addresses to external addresses.
3. Inbound services shall be negotiated on a case by case basis.
4. All workforce members connecting to the Ulster County WAN shall sign the Ulster County IT Security Policy before connectivity is established.

Firewall Controls

1. Networks containing systems and applications with EPHI shall implement perimeter security and access control with a firewall.
2. Firewalls shall be configured to support the following minimum requirements:
   a) Limit network access to only authorized workforce members and entities
   b) Limit network access to only legitimate or established connections
   c) Console and other management ports shall be appropriately secured or disabled
3. The configuration of firewalls used to protect networks containing EPHI based systems and applications shall be reviewed and approved by UCIS.

Procedure Responsibilities:

Workforce Member Responsibilities

All workforce members that transmit EPHI outside the Ulster County WAN are responsible for ensuring the information is safeguarded by using encryption when using the Internet or a wireless connection.

UCIS IT Support Responsibilities

UCIS is responsible for the perimeter security architecture, its resources, its periodic auditing, and testing.

Procedure: HIPAA/HITECH Compliance
Topic: *User Access Management*

HIPAA Regulation:

• *Workforce security*	§164.308(a)(3)	addressable
• *Workforce Authorization and/or supervision*	§164.308(a)(3)	addressable
• *Workforce clearance procedure*	§164.308(a)(3)	addressable
• *Workforce Termination procedure*	§164.308(a)(3)	addressable
• *Information access management*	§164.308(a)(4)	addressable
• *Access authorization*	§164.308(a)(4)	addressable
• *Access establishment and modification*	§164.308(a)(4)	addressable
• *Access control*	§164.312(a)(1)	required
• *Integrity*	§164.312(c)(1)	addressable
• *Emergency access procedure*	§164.312(a)(1)	addressable

Purpose:

The purpose of this procedure is to establish rules for authorizing access to the computing network, applications, workstations, and to areas where electronic protected health information (EPHI) is accessible. The HIPAA covered components shall ensure that only workforce members who require access to EPHI for work related activities shall be granted access and when work activities no longer require access, authorization shall be terminated.

In section §160.103 of the HIPAA Privacy Rule, the “workforce” is defined as “employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.”

Description:

Management and Access Control
Only the workforce member’s manager or an appropriate designee can authorize access to the Ulster County information systems.

Access to the information system or application may be revoked or suspended, consistent with Ulster County policies and practice, if there is evidence that an individual is misusing information or resources. Any individual whose access is revoked or suspended may be subject to disciplinary action or other appropriate corrective measures.

Minimum Necessary Access

Ulster County shall ensure that only workforce members who require access to Electronic Protected Health Information (EPHI) are granted access.

Each manager or supervisor is responsible for ensuring that the access to EPHI granted to the workforce member is the minimum necessary access required for each work role and responsibilities.

If the workforce member no longer requires access, it is the responsibility of the manager or appropriate designee to complete the necessary process to terminate access.

Granting Access to EPHI

Screen Workforce Members Prior to Access

The manager or designee shall ensure that information access is granted only after first verifying that the access of a workforce member to EPHI is appropriate.

Sign Security Acknowledgement

Prior to being issued a User ID or logon account to access any EPHI, each workforce member shall sign the Ulster County *Security Rule Policy and Procedures Acknowledgement* before access is granted to the network or any application that contains EPHI, and thereafter shall comply with all Ulster County security policies and procedures.

Security Awareness Prior to Getting Access

Before access is granted to any of the various systems or applications that contain EPHI, the manager or appropriate designee shall ensure that workforce members are trained to a minimum standard including:

1. Proper uses and disclosures of the EPHI stored in the systems or application
2. How to properly log on and log off the systems or application
3. Protocols for correcting user errors
4. Instructions on contacting a designated person or help desk when EPHI may have been altered or destroyed in error
5. Reporting a potential or actual security breach

Management/Supervisor Approval Implement
the following procedures:

1. User IDs or logon accounts can only be assigned with management approval or by an appropriate designee.
2. Managers or their designees are responsible for requesting the appropriate level of access for staff to perform their job function.
3. All requests regarding user IDs or computer system access for workforce members are to be communicated to the system administrator. All requests shall be made using the County's electronic IT ticketing system, which can be accessed from the County's intranet portal.
4. System administrators are required to process only those requests that have been authorized by managers or their appropriate designees.

5. A written or electronic record of the authorized request is to be retained by the system administrator for a period of time the approved user has access, plus a minimum of one year.

Granting Access in an Emergency

Management has the authority to grant emergency access for workforce members who have not completed the normal HIPAA access requirements if:

1. Management declares an emergency or is responding to a natural disaster that makes client information security secondary to personnel safety.
2. Management determines that granting immediate access is in the best interest of the client.
3. If emergency access is granted, the manager shall review the impact of emergency access and document the event within 24 hours of it being granted.
4. After the emergency event is over, the user access shall be removed or the workforce member shall complete the normal requirements for being granted access.

Termination or Suspension of Access

Department managers or their designated representatives are responsible for terminating a workforce member's access to EPHI in these circumstances:

1. If management has evidence or reason to believe the individual is using information systems or resources in a manner inconsistent with HIPAA Security Rule policies.
2. If the workforce member or management has reason to believe the user's password has been compromised.
3. If the workforce member resigns, is terminated, suspended, retires, or is away on unapproved leave.
4. If the workforce member's work role changes and system access is no longer justified.

If the workforce member is on a leave of absence and the user's system access will not be required for more than four weeks, management shall suspend the user's account until the workforce member returns from their leave of absence.

Modifications to Access

If a workforce member transfers to another department or changes their work role within the same department, the workforce member's new manager or supervisor is responsible for evaluating the member's current access and for requesting new access to EPHI commensurate with the workforce member's new work role and responsibilities.

Ongoing Compliance for Access

In order to ensure that workforce members only have access to EPHI when it is required for their job function, the following actions shall be implemented:

1. Every new user ID or logon account that has not been used after 30 consecutive calendar days since creation shall be investigated to determine if the workforce member still requires access to the EPHI.
2. At least every six months, UCIS is required to send managers or appropriate designees:
    - A list of all workforce members for all applications
    - A list of all workforce members and their access rights for all shared folders that contain EPHI
    - A list of all workforce members approved for access to Virtual Private Network (VPN)
3. The managers or their designees shall then notify UCIS Customer Support of any workforce members who no longer require access.

Procedure Responsibilities:

Manager and Supervisor Responsibilities

1. Ensure that the access to EPHI granted to each of their workforce members is the minimum necessary access required for each such workforce member's work role and responsibilities.
2. In order to protect the security of the file server from malicious intent or unauthorized use by non-employees, each department manager is responsible to report employee termination (voluntary and non-voluntary), employee suspension, or employees expected to be on leave for more than four weeks (medical, workers comp, etc.) to UCIS within 24 hours. UCIS will disable computer access upon notification.
3. Request termination of access if the workforce member no longer requires access.
4. Validate new User IDs or logon accounts that are not used within 30 days of creation and provide UCIS with the information.
5. Review semi-annual user and folder access reports and the VPN access reports prepared by UCIS and verify to determine if the workforce members still require access to EPHI.
6. Ensure that members of the workforce have signed the County's security agreement and are properly trained before approving access to EPHI.
7. Follow the appropriate security procedures when granting emergency access with support from UCIS as required.

UCIS IT Support Responsibilities

1. Immediately upon written notification, remove or modify a workforce member's access to EPHI.
2. Provide management with a report that identifies new User IDs or logon accounts not used within 30 days of creation.
3. Provide management with a semi-annual report documenting workers with access to EPHI, and requesting verification that access is still required to fulfill the worker's job functions.
4. When required, support management with the appropriate security procedures for granting emergency access.

Workforce Member Responsibilities

Each user of a system or application that contains EPHI shall:

1. Read and sign the Ulster County *Security Rule Policy and Procedures Acknowledgement*.
2. Follow all Information Security policies and requirements.
3. Complete HIPAA Privacy and Security training.
4. Immediately report all security incidents to their supervisor or other appropriate manner consistent with Ulster County policy.
5. Any employee who has a user account to access computer resources must take necessary precautions to keep confidential the password associated with that user account. Employees who feel that other individuals have knowledge of their password must report this to their supervisor and UCIS Customer Support, so the password can be changed.

Procedure: HIPAA/HITECH Compliance
Topic: *Virtual Private Network (VPN)*

Purpose:

The purpose of this procedure is to provide guidelines for Remote Access IPSec or L2TP Virtual Private Network (VPN) connections to the Ulster County network.

This procedure applies to all Ulster County employees, contractors, consultants, temporaries, and other workers including all personnel affiliated with third parties utilizing VPNs to access the Ulster County network. This policy applies to implementations of VPN that are directed through an IPSec Concentrator.

Procedure Description / Responsibilities:

Approved Ulster County employees and authorized third parties (customers, vendors, etc.) may utilize the benefits of VPNs, which are a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees. Further details may be found in the ***Remote Access Policy***.

In addition:

1. It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to Ulster County internal networks.
2. VPN use is to be controlled using either a one-time password authentication such as a token device or a public/private key system with a strong passphrase.
3. When actively connected to the corporate network, VPNs will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped.
4. Dual (split) tunneling is NOT permitted; only one network connection is allowed.
5. VPN gateways will be set up and managed by Ulster County network operational groups.
6. All computers connected to Ulster County internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the County standard (contact UCIS Customer Support for latest information); this includes personal computers.
7. VPN users will be automatically disconnected from Ulster County's network after thirty minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.
8. The VPN concentrator is limited to an absolute connection time of 24 hours.
9. Users of computers that are not Ulster County owned equipment must configure the equipment to comply with Ulster County's VPN and Network policies.
10. Only UCIS-approved VPN clients may be used.

11. By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of Ulster County's network, and as such are subject to the same rules and regulations that apply to Ulster County-owned equipment, i.e., their devices must be configured to comply with Ulster County/UCIS Security Policies and Procedures.

Procedure: HIPAA/HITECH Compliance

Topic: *Wireless Communication*

Purpose:

This procedure prohibits access to Ulster County networks via unsecured wireless communication mechanisms. Only wireless systems that meet the criteria of this policy or have been granted an exclusive waiver by UCIS are approved for connectivity to Ulster County networks.

This procedure covers all wireless data communication devices (e.g., personal computers, mobile devices/smartphones phones, etc.) connected to any of Ulster County's internal networks. This includes any form of wireless communication device capable of transmitting packet data. Wireless devices and/or networks without any connectivity to Ulster County's networks do not fall under the purview of this policy.

Procedure Description / Responsibilities:

Register Access Points and Cards
All wireless Access Points/Base Stations connected to the County network must be registered and approved by UCIS.

Approved Technology
All wireless LAN access must use County-approved vendor products and security configurations.

VPN Encryption and Authentication
All computers with wireless LAN devices must utilize a County-approved virtual Private Network (VPN) configured to drop all unauthenticated and unencrypted traffic. To comply with this policy, wireless implementations must maintain point to point hardware encryption of at least 256 bits. All implementations must support a hardware address that can be registered and tracked, i.e., a MAC address. All implementations must support and employ strong user authentication which checks against an external database such as TACACS+, RADIUS, or something similar.

Setting the SSID
The SSID shall be configured so that it does not contain any identifying information about the organization, such as the company name, division title, employee name, or product identifier.

Procedure: HIPAA/HITECH Compliance
Topic: *Workstation Security*

HIPAA Regulation:

• *Access control and validation*	§164.312(a)(1)	required
• *Workstation use*	§164.310(b)	required
• *Workstation security*	§164.310(c)	required
• *Automatic log off*	§164.312(a)(1)	addressable

Purpose:

The purpose of this procedure is to establish rules for securing workstations that access electronic protected health information (EPHI). Since EPHI can be portable, this policy requires workforce members to protect EPHI at Ulster County worksites and all other locations.

Description:

Ulster County shall implement safeguards to prevent unauthorized access to EPHI through workstations and to protect EPHI from any intentional or unintentional use or disclosure.

Workstation Security Controls
All workstations used by workforce members with access to EPHI shall be set to automatically lock the computer when it is left unattended, requiring the user to enter a password to unlock the workstation. The standard setting for the computer to lock after a period of inactivity is not to exceed 10 minutes.

Workforce members shall manually lock their workstation computer using the Ctrl-Alt-Delete key combination when the computer is left unattended for any period of time.

Workforce members shall ensure that observable confidential information is adequately shielded from unauthorized disclosure and access on computer screens. At each site, every effort shall be made to ensure that confidential information on computer screens is not visible to unauthorized persons.

Workforce members who work from home or other non-office sites shall follow the above workstation security controls to safeguard EPHI access or viewing by any unauthorized individual.

Workforce members shall protect printed versions of EPHI that have been transmitted via fax or multi-use machines by promptly removing documents from shared devices.

Whenever possible, confidential documents are to be placed in locked cabinets or drawers when left unattended.

Procedure Responsibilities:

Supervisor and Manager Responsibilities

1. Control workforce member access to EPHI as per the ***User Access Management Policy***.
2. Take appropriate corrective action if any workforce member knowingly violates the security of workstation use.
3. Ensure that the automatic lock is functioning on all workstations.
4. Ensure that all workforce members are locking their workstations when they are left unattended.
5. Ensure that all confidential information is not viewable by unauthorized persons at workstations in offices under their management.

Workforce Member Responsibilities

1. Lock their computer when it is left unattended for any period of time.
2. Do not change or disable the automatic inability lock on their workstation.
3. Ensure that all confidential information in their workstation is not viewable or accessible by unauthorized persons.
4. When working from home or other non-office work sites, protect EPHI from unauthorized access or viewing.

UCIS IT Support Responsibilities

1. When installing new workstations, set the computer to automatically lock after the recommended period of inactivity, which is not to exceed 10 minutes.

Appendix A: Definitions

Term	Definitions
Business Associate	A Contractor who completes a function or activity involving the use or disclosure of protected health information (PHI) or electronic protected health information (EPHI) on behalf of a HIPAA covered component. Services that Business Associate (BA) contractors provide include: Claims processing or administration; data analysis, processing and/or administration; data analysis, processing and/or administration; utilization review; quality assurance; billing; benefit management; document destruction; temporary administrative support; legal; actuarial; accounting; consulting; information technology (IT) support. The BA contractor does not deliver health care services to clients of the HIPAA covered component.
Breach	An impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised.
Device	A unit of hardware, inside or outside the case or housing for the essential computer functions (the processor, memory, and data paths). A device is capable of providing input, receiving output, or both.
Disposal	The removal or destruction of electronic protected health information from electronic media.
DMZ (demilitarized zone)	Any untrusted network connected to, but separated from, Ulster County's network by a firewall, used for external (Internet/partner, etc.) access from within Ulster County, or to provide information to external parties.
Electronic Protected Health Information (EPHI)	Protected Health Information (PHI) is health information that a covered entity creates or receives that identifies an individual, and relates to: The individual's past, present, or future physical or mental health or condition; the provision of health care to the individual; or the past, present, or future payment for the provision of health care to the individual. EPHI is such information in electronic format such as: information system applications; internet, intranet and extranet; email; USB drives; computer screens; laptops; storage devices (magnetic tapes, floppy disks, CDs, optical devices).
Email	The electronic transmission of information through a mail protocol such as SMTP. Programs such as Eudora and Microsoft outlook use SMTP.
Encryption	A method of scrambling or encoding electronic data to prevent unauthorized access. Only individuals with access to a password or key can decrypt (unscramble) and use the data.
Facility	A building, owned or leased, in which the workforce accesses Electronic Protected Health Information (EPHI).
Firewalls	Special computer programs and hardware that are set up on a network to prevent an intruder from stealing or destroying data.

Forwarded email	Email re-sent from internal networking to an outside point.
Hard Drive	An information storage device that contains electronic information and software programs on a computer. Information stored on the hard drive [or local (C:) drive] is not backed up on the network.
UCIS	Ulster County Information Services
IT	Information Technology. Refers to the Management Information Systems department or the Information Technology staff at Ulster County.
Jailbreak	To remove the limitations imposed by the manufacturer. This gives access to the operating system, thereby unlocking all its features and enabling the installation of unauthorized software.
Key pads - cipher locks	Door locks that require a combination of numbers entered into a pad in order to unlock the door.
Local (C:) drive	In the context of this policy, the individual user's hard drive where electronic information can be stored (saved), rather than stored on the organization-wide network. The local (C :) drive should not be used to store EPHI.
Malicious software or malware	A type of software that includes ways of attacking data integrity, the system itself or the confidentiality of the data. Malicious software includes viruses, virus variants, worms, hoaxes, and Trojan horses.
Media reuse	A device such as a computer hard drive that contained data (information) that is being reused to contain new data.
Modem	A device that enables data to be transmitted over telephone or cable lines. It translates telephone tones to allow for the multiplexing of data (information) across the telephone network, generally in order to access the internet.
Network	A group of computers (workstations) and associated devices connected by a communications channel to share information files and other resources between multiple workforce members.
Network closets	Storage area of network equipment such as hubs, routers, switches, racks, cables, and sometimes has telephone equipment, at a HIPAA covered component facility.
Networked computer/ workstation	A workstation computer that uses server resources. It is usually connected to a Local Area Network (LAN), which shares the resources of one or more large computers.
Payload	Harmful code delivered by a software virus.
Perimeter Security	Security that protects the network and its component server computers from attack or intrusion.
Portable media	Devices carried or moved with ease that can contain electronic protected health information (EPHI). The most common are: laptops; CDs; USB drives (or memory sticks); and personal digital assistants (PDAs), including smartphones or Blackberries.

Risk Assessment	A process of assessing those factors that could affect confidentiality, availability, and integrity of key information assets and systems. HIPAA covered components are responsible for ensuring the integrity, confidentiality, and availability of EPHI and equipment that contains it, while minimizing the impact of security procedures and policies upon business productivity.
Secure Channel	Out-of-band console management or channels using strong encryption according to the ***Acceptable Encryption Policy***. Non-encrypted channels must use strong user authentication (one-time passwords).
Sensitive information	Information is considered sensitive if it can be damaging to Ulster County or its customers' dollar value, reputation, or market standing.
Server	A computer or device on a network that managers network resources.
Server Room	The room where all the server computers are housed.
Strong Passwords	A password that is difficulty to guess by both humans and computer programs, effectively protecting data from unauthorized access. A strong password consists of at least six characters that are a combination of letters, numbers and symbols (@, #, $, %, etc.) if allowed. Strong passwords contain the maximum number of characters allowed. Passwords are typically case-sensitive so a strong password contains letters in both uppercase and lowercase. Strong passwords also do not contain words that can be found in a dictionary or any part of the user's own name.
Transmitting	The act of sending a message or data using an electronic medium.
Trojan or Trojan horse	A Trojan or Trojan horse is a computer program generally designed to impact the security of a network system. The Trojan is usually disguised as something else (a benign program) or masquerades as a legitimate file that the user would expect to see, or want to load, on the network system. The payload of a Trojan is usually delivered as soon as it is opened with devastating results. Trojans often create "back doors" that allow access into a secure network. A hacker can then gain access to the secure network. Trojans are most often delivered as an attachment to a seemingly innocent chain email.
Unauthorized Disclosure	The intentional or unintentional revealing of restricted information to people who do not have a need to know that information.
Un-trusted Network	Any network firewalled off from the corporate network to avoid impairment of production resources from irregular network traffic (lab networks), unauthorized access (partner networks, the Internet, etc.) or anything else identified as a potential threat to those resources.
USB drive, USB flash drive, thumb drive, or memory stick	A small, portable device that plugs into a workstation computer's USB port and functions as a portable hard drive with extra storage capacity. USB devices are easy to use, small enough to be carried in a pocket, and can plug into any workstation computer with a USB drive.

User	For the purposes of this document, any workforce member (permanent or temporary), contractor, consultant, vendor, volunteer, student, or other person who uses, maintains, manages, or is otherwise given access privileges to system resources.
User ID or logon	An identification code issued for access privileges which identifies the user to IT systems.
Virtual Private Network (VPN)	A secure, encrypted network connection between two or more devices across the public internet or other shared network. It allows workstation computers at different locations to securely communicate with each other.
Virus	A computer program that copies itself into another program, sectors on a drive, or into items that support scripts. A virus may unleash a payload. Payloads can damage files, corrupt hard drives, display messages, or open other files. Typically, the payload is delivered when a certain condition occurs, such as when the date on the workstation reaches a particular day.
Workforce/ workforce member	In the HIPAA Privacy rule, the term "workforce" is defined as "employees, volunteers, trainees, and other persons who conduct, in the performance of work for a HIPAA covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity." Workforce members include supervisors, managers, and staff.
Workstation	A laptop or desktop computer, or any other device that performs computer functions.
Worm	A type of virus that finds vulnerable computer systems and then copies itself into those systems. The most frequent copying methods are from email distribution lists, email signature scripts, and shared folders on the network. A typical worm payload makes the workstation more susceptible to other malicious viruses.

Appendix B: Security Rule Policy and Procedures Acknowledgement

I understand that while performing my official duties I may have access to protected health information. I understand that:

- Protected health information is individually identifiable health information that is created, maintained, or used by Ulster County.
- Special precautions are necessary to protect this type of information from unlawful or unauthorized access, use, modification, disclosure, or destruction.

The undersigned acknowledges receiving a copy of Ulster County Health Insurance Portability and Accountability Act (HIPAA) Security Rule Policy and Procedures:

Print full name (first, middle initial, last)	***Signature***
Department	***Date signed***

ULSTER COUNTY
NOTICE OF PRIVACY PRACTICES

This notice describes the privacy practices of Ulster County and the privacy rights of the people we serve. It will describe how information about you may be used and disclosed and how you can get access to this information.

The Health Insurance Portability and Accountability Act (HIPAA) Privacy rule DOES NOT CHANGE the way you get services from Ulster County, or the privacy rights you have always had under federal and state laws. The Privacy rule adds some details about how you can exercise your rights.

PLEASE REVIEW THIS NOTICE CAREFULLY.

Our Privacy Commitment to You:

Ulster County provides many different services to you. We understand that information about you and your family is personal. We are committed to protecting your privacy and sharing information only with those who need to know and are allowed to see the information to assure quality services for you. Ulster County is required by law to maintain the privacy of your health information and to provide you with notice of its legal duties and privacy practices with respect to your health information. This notice tells you how Ulster County uses and discloses information about you. It describes your rights and what Ulster County's responsibilities are concerning information about you. When we use the word "you" in this Notice, we also mean your personal representative. Depending on your circumstances and in accordance with state law, this may mean your guardian, your health care proxy, or your involved parent, spouse, or involved adult family member.

If you have questions about any part of this notice or if you want more information about the privacy practices at Ulster County, please contact:

Clint Johnson, Privacy Officer for Ulster County
Address: 244 Fair Street, Kingston, NY 12401
Phone: 845-340-3685
E-mail: **cjoh@co.ulster.ny.us**

Or Department Head that is utilizing this notice:

Who will follow this Notice:

All people who work for Ulster County will follow this notice. This includes employees, persons Ulster County contracts with who are authorized to enter information in your record or need to review your record to provide services to you, and volunteers who Ulster County allows to assist you.

What information is protected:

All information that we create or keep that relates to your health or care and treatment, including but not limited to your name, address, birth date, social security number, your medical information, your service or treatment plan, and other information (including photographs or other images) about your care in our programs, is considered protected information. In this Notice, we refer to protected information as protected health information or "PHI". We create and collect information about you and we keep a record of the care and services you receive though this agency. The information about you is kept in a record; it may be in the form of paper documents in a chart or on a computer. We refer to the information that we create, collect, and keep as a "record" in this Notice.

Your Health Information Rights:

Unless otherwise required by law, your record is the physical property of Ulster County, but the information in it belongs to you and you have the right to have your information kept confidential. You have the following rights concerning your PHI:

- You have a right to see or inspect your PHI and obtain a copy of the information. Some exceptions apply, such information compiled for use in court or administration proceedings. NOTE: Ulster County requires you to make your request for records in writing to the Privacy Officer You may request copies in paper format or in an electronic form such as a CD, portable device, or memory stick. In some instances, we may charge you for copies.
- If we deny your request to see your information, you have the right to request a review of that denial. The Privacy Officer will appoint a licensed health care professional to review the record and decide if you may have access to the record.
- You have the right to ask Ulster County to change or amend information that you believe is incorrect or incomplete. We may deny your request in some cases, for example, if the record was not created by Ulster County or if after reviewing your request, we believe the record is accurate and complete.
- You have the right to request a list of the disclosures that Ulster County has made of your PHI. The list, however, does not include certain disclosures, such as those made for treatment, payment, and health care operations, or disclosures made to you or made to others with your permission.

- You have the right to request a restriction on uses or disclosures of your health information related to treatment, payment, health care operations, and disclosures to involved family. Ulster County, however, is not required to agree to your request.
- You have the right to request that Ulster County communicates with you in a way that will help keep your information confidential. You may request alternate ways of communication with you or request that communications are forwarded to alternative locations.
- You have the right to limit disclosures to insurers if you have paid for the service completely out of pocket.
- You will be notified if there is a breach of unsecured PHI containing your information; we are required by federal law to provide notification to you.
- To request access to your clinical information or to request any of the rights listed here, you may contact:

  Clint Johnson, Privacy Officer, or the Department Head utilizing this notice.

  Address: 244 Fair Street, Kingston, NY 12401

  Phone: 845-340-3685

  E-mail: cjoh@co.ulster.ny.us

We will require you to submit your requests in writing to the Privacy Officer or the Department Head utilizing this notice.

NOTE: Other regulations may restrict access to HIV/AIDS information, federally protected education records, and federally protected drug and alcohol information. See any special authorizations or consent forms that will specify what information may be released and when, or contact the Privacy Officer listed above.

Our Responsibilities to You:

We are required to:

- Maintain the privacy of your information in accordance with federal and state laws.
- Give you this Notice that tells you how we will keep your information private.
- Tell you if we are unable to agree to a limit on the use or disclosure that you request.
- Carry out reasonable requests to communicate information to you by special means or at other locations.
- Get your written permission to use or disclose your information except for the reasons explained in this notice.
- We have the right to change our practices regarding the information we keep. If practices are changed, we will tell you by giving you a new notice. Notices will be posted on our website: http://ulstercountyny.gov/ or the Department utilizing this notice.

How Ulster County Uses and Discloses Your Health Information:

Ulster County may use and disclose information without your permission for the purposes described below. For each of the categories of uses and disclosures, we explain what we mean and offer an example. Not every use or disclosure is described, but all of the ways we will use or disclose information will fall within these categories.

- **Treatment:** Ulster County will use your information to provide you with treatment and services. We may disclose information to doctors, nurses, psychologists, social workers, and other Ulster County personnel, volunteers, or interns who are involved in providing your care. For example, involved staff may discuss your information to develop and carry out your treatment or service plan and other Ulster County staff may share your information to coordinate different services you need, such as medical tests, respite care, transportation, etc. We may also need to disclose your information to other providers outside of Ulster County who are responsible for providing you with services.
- **Payment:** Ulster County will use your information so that we can bill and collect payment from you, a third party, an insurance company, Medicare or Medicaid, or other government agencies. For example, we may need to provide your health care insurer with information about the services you received in our agency or through one of our programs so they will pay us for the services. In addition, we may disclose your information to receive prior approval for payment for services you may need.
- **Health Care Operations:** Ulster County will use clinical information for administrative operations. These uses and disclosures are necessary to operate Ulster County programs and to make sure all individuals receive appropriate, quality care. For example, we may use information for quality improvement to review our treatment and services and to evaluate the performance of our staff in serving you.

We may also disclose information to clinicians and other personnel for on-the-job training. We will share your health information with other Ulster County staff for the purposes of obtaining legal services from our attorneys, conducting fiscal audits, and for fraud and abuse detection and compliance through our Compliance Program. We may also disclose information to our business partners who need access to the information to perform administrative or professional services on our behalf.

Other Uses and Disclosures that Do Not Require your Permission:

In addition to treatment, payment, and health care operations, Ulster County will use your information without your permission for the following reasons:

- When we are **required to do so by federal or state law**.
- For **public health reasons**, including prevention and control of disease, injury or disability, reporting births and deaths, reporting child abuse or neglect, reporting reactions to medication or problems with products, and to notify people who may have been exposed to a disease or are at risk of spreading the disease.
- To report **domestic violence and adult abuse or neglect** to government authorities if necessary to prevent serious harm.
- For **health oversight activities**, including audits, investigations, surveys and inspections, and licensure. These activities are necessary for government to monitor the health care system, government programs, and compliance with civil rights laws. Health oversight activities do not include investigations that are not related to the receipt of health care or receipt of government benefits in which you are the subject.
- For **judicial and administrative proceedings**, including hearings and disputes. If you are involved in a court or administrative proceeding we will disclose information if the judge or presiding officer orders us to share the information.
- For **law enforcement purposes**, in response to a court order or subpoena, to report a possible crime, to identify a suspect or witness or missing person, to provide identifying data in connection with a criminal investigation, and to the district attorney in furtherance of a criminal investigation of client abuse.
- Upon your death, to **coroners or medical examiners** for identification purposes or to determine cause of death, and to **funeral directors** to allow them to carry out their duties.
- To organ procurement organizations to accomplish cadaver, eye, tissue, or **organ donations** in compliance with state law.
- For **research** purposes when you have agreed to participate in the research and the Compliance Committee has approved the use of the clinical information for the research purposes.
- To **prevent or lessen a serious and imminent threat** to your health and safety or someone else's.
- To authorized federal officials for intelligence and other **national security** activities authorized by law or to provide **protective services to the President** and other officials.
- To **correctional institutions** or **law enforcement officials** if you are an inmate and the information is necessary to provide you with health care, protect your health and safety or that of others, or for the safety of the correctional institution.
- To **governmental agencies that administer public benefits** if necessary to coordinate the covered functions of the programs.

Uses and Disclosures that Require Your Agreement:

Ulster County may disclose information to the following persons if we tell you we are going to use or disclose it and you agree or do not object:

- To **family members and personal representatives** who are involved in your care if the information is relevant to their involvement and to notify them of your condition and location.
- To **disaster relief organizations** that need to notify your family about your condition and location should a disaster occur.
- For **fundraising** purposes, we may disclose information to a charitable program that assists us in fundraising with your permission. You have the right to refuse or opt out if you previously agreed to communications regarding fundraising.
- For **marketing** of health- related services, we will not use your health information for marketing communications without your permission.
- To disclose **psychotherapy** notes.

Authorization Required For All Other Uses and Disclosures:

- For all other types of uses and disclosures not described in this Notice, Ulster County will use or disclose information only with a written authorization signed by you that states who may receive the information, what information is to be shared, the purpose of the use or disclosure and an expiration for the authorization. Written authorizations are always required for the sale of PHI and use and disclosure for marketing purposes, such as agency newsletters and press releases.

  Note: If you cannot give permission due to an emergency, Ulster County may release information in your best interest. We must tell you as soon possible after releasing the information.

  You may revoke your authorization at any time. If you revoke your authorization in writing we will no longer use or disclose your information for the reasons stated in your authorization. We cannot, however, take back disclosures we made before you revoked and we must retain information that indicates the services we have provided to you.

Changes to this Notice:

- **We reserve the right to change this Notice**. We reserve the right to make changes to terms described in this Notice and to make the new notice terms effective to all information that Ulster County maintains. We will post the new notice with the effective date on our website at http://ulstercountyny.gov/ and will make this notice available in all departments that utilize this notice. In addition, we will offer you a copy of the revised notice at your next scheduled service planning meeting.

Complaints:

If you believe your privacy rights have been violated, you may file a complaint with:

- Clint Johnson, Privacy Officer, or the Department Head utilizing this notice
  Address: 244 Fair Street, Kingston, NY 12401
  Phone: 845-340-3685
  E-mail: cjoh@co.ulster.ny.us

- Or, you may contact the Director of Office for Civil Rights, U.S. Department of Health and Human Services, 200 Independence Avenue, S.W., Room 509F HHH Bldg., Washington, D.C. 20201, Secretary of the Department of Health and Human Services. You may call them at (877) 696-6775 or write to them at 200 Independence Ave. S.W., HHH Building Room 509H, Washington DC, 20201.

- You may file a grievance with the Office of Civil Rights by calling or writing Region II – US Department of Health and Human Services, Jacob Javits Federal Building, 26 Federal Plaza, Suite 3312, New York, New York 10278, Voice Phone (800) 368-1019, FAX (212) 264-3039, TDD (800) 537-7697.

All complaints must be submitted in writing. **You will not be penalized for filing a complaint.**