



URMC/Strong Health HIPAA Privacy Training Module

POLICY SUMMARY: OP2

(for full policy, refer to <http://intranet.URMC.Rochester.Edu/Policy/HIPAA/>)

Mitigation

URMC/Strong Health will mitigate (lessen), to the extent practicable, any known harmful effect of a use or disclosure of protected health information (PHI) either by URMC/Strong Health or a business associate in violation of:

- URMC/Strong Health privacy policies, or
- Privacy regulations adopted under HIPAA

Who needs to follow this policy?

Anyone who becomes aware of a *privacy violation that has caused a harmful effect to an individual.*

What should a member of the workforce do if he/she suspects harm has been done by inappropriate disclosure of PHI?

Immediately contact the Privacy Officer for that entity who will coordinate efforts to reduce that harm.

What steps will be taken to lessen the harm that might have occurred?

The Privacy Officer will:

- attempt to prevent further disclosure by those responsible (if the offending person is a member of the URMC/Strong Health workforce or a Business Associate) and
- take action against those individuals, up to and including sanctions, as appropriate.

Will the patient or family member be notified that their PHI has been disclosed inappropriately and the steps that have been taken to stop further disclosure?

The decision to inform patients will be made on a case-by-case basis, depending on what was disclosed, to whom, by whom and what harm may have been caused.

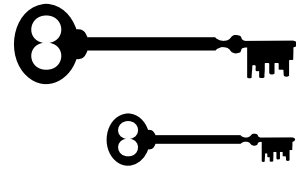
Sample Situations: Mitigation

After Mrs. Y gives her son's information to the intake clerk, she sits down in the crowded waiting room while her insurance information is being verified. After a few minutes, the clerk says to Mrs. Y in a loud voice, "No need to get up; just want to check that your address is 123 Parkson Ave, right?" The clerk's supervisor hears this and looks up to see Mrs. Y looking very angry as she walks to the clerk's desk to speak to her in a low voice.

- Obviously Mrs. Y is upset, but the action of the clerk does not appear to have caused a harmful effect to the patient. However, the supervisor should speak with the clerk regarding appropriate use of PHI.

Sherilyn receives a phone call from a newspaper reporter who wants to confirm she is pregnant with quintuplets. The reporter wants to run the story so the community will 'rally' to help her and her husband when the quintuplets are born. She is furious that this news has gotten to the press and assumes her doctor's office has called the newspaper. Upon investigation, the Obstetrician discovers that when the Nurse Practitioner congratulated Sherilyn, several staff overheard her and joined in with their best wishes. One of the staff members knows that Sherilyn and her husband will have a difficult time supporting quints, so she notified the newspaper anonymously in an effort to get them some help.

- Although the staff member may have been well intended, this is a definite breach of the HIPAA regulations and URM/Strong Health policies. The Privacy Officer must be notified and work with the Obstetrician and the staff member who called the newspaper to correct the situation. The staff member is subject to disciplinary actions up to and including termination from her job. Sherilyn's Department Head/supervisor will follow up with her after the intervention as appropriate to lessen any harmful effects.



URMC/Strong Health HIPAA Privacy Training Module

POLICY SUMMARY: OP4

(for full policy, refer to <http://intranet.URMC.Rochester.Edu/Policy/HIPAA>)

Designation of Privacy Official/Contact Person/Office

As a covered entity, URMC/Strong Health must designate a Privacy Official to be responsible for the development and implementation of privacy policies and procedures. The following policy:

- Identifies the Privacy Officers for URMC/Strong Health.
- Identifies contact persons for patient, employee, volunteer or other inquiries, requests, questions and complaints concerning privacy matters.
- Outlines the duties, responsibilities and reporting relationships of the privacy officers and the contact persons.

Who needs to follow this policy?

The University of Rochester Medical Center/Strong Health is considered a 'covered entity' under the HIPAA Privacy Rule. As such, URMC/Strong Health must designate a Privacy Officer to be responsible for the development and implementation of Privacy policies and procedures.

What does a Privacy Officer do?

They are responsible for overseeing all the work that relates to creating HIPAA policies, conducting training, monitoring compliance, receiving complaints and applying sanctions (penalties) to those who do not follow the laws and policies.

Privacy Officers provide information to you about HIPAA and how it applies to the different parts of URMC/Strong Health.

They also work with information systems (computer) staff to develop a secure system for clinical information and work with researchers to make sure research guidelines are followed.

Privacy Officers are also responsible for keeping up-to-date on changes in the laws and standards that relate to HIPAA and keeping the organization informed so changes can be made in policies and training.

Since URMC/Strong Health is such a large organization, several people share the Privacy Officer's responsibilities. Please go to the link below for a current listing of Privacy Officers:

<http://intranet.urmc.rochester.edu/HIPAA/FAQsResources/Officers.asp>

Sample Situations: Designation of Privacy Official/Contact Person/Office

Ms. K was unhappy with a loud conversation that took place at the Nurses' Station after 10 p.m. last night. She also thought she might have heard her name being spoken quite loudly during this conversation. She has just asked the Dietary Aide to whom she should complain. What does the Dietary Aide tell her?

- The Aide can refer her to the Nurse Manager who will handle the problem. If Ms. K does not want to talk to the Nurse Manager, she could call the Strong Health Integrity Hotline at 585-756-8888 to contact the Privacy Officer.

Kelisha overheard two clerks talking about covering for each other during vacations. One clerk offered to share her password with the other clerk just in case she needed to get into her computer while she was away. Kelisha called the Privacy Officer to report this. Was this action correct?

- It was not incorrect, but whenever possible, the violation or potential violation should be handled where it occurred. Kelisha should have spoken to her supervisor to ask for assistance, or if she knew the clerks, could have reminded them that passwords are not to be shared with anyone.

When Jorge arrives to take Mrs. F. to physical therapy, two of her family members ask him the name of the Privacy Officer; they have a complaint regarding their impression of the general lack of privacy in the nursing home. They feel Mrs. F's treatment is not being handled in the strictest confidence and want it corrected immediately. How should Jorge help them?

- He can direct them to the lead person on that floor who can assist the family.



URMC/Strong Health HIPAA Privacy Training Module

POLICY SUMMARY: OP5

(for full policy, refer to <http://intranet.URMC.Rochester.Edu/Policy/HIPAA>)

Sanctions

URMC/Strong Health will review all reported violations of URMC/Strong Health's privacy policies or the Privacy regulation and will impose sanctions on responsible members of the workforce as indicated.

Who needs to follow this policy?

All URMC/Strong Health workforce members.

Who will determine and impose sanctions when patient privacy has been violated?

The Privacy Officer will work with representatives from Human Resources, the Medical Director, Associate Dean for Graduate Medical Education, senior leadership and/or the Office of Counsel, whomever is appropriate for that violation.

What types of sanctions will be imposed?

The level of sanction will correspond to the seriousness of the violation and may include, but is not limited to:

1. Termination
2. Loss of medical staff or practice privileges

Other disciplinary actions may include counseling, probation, focused auditing or reporting to legal or regulatory authorities.

What factors, if any, will be taken into consideration when a violation has occurred?

The Privacy Officer and URMC/Strong Health management may consider, among other things, whether or not the violation:

1. Is a single incident.
2. Is a repeat incident.
3. Was committed with the willful intent to do harm.

What kind of documentation will be kept on violations and sanctions?

The Privacy Office will retain all documentation relating to the incident for six years.

Are there exceptions to when sanctions will be imposed?

Yes, there will be no sanctions when:

1. A workforce member is acting as a whistleblower (see [Policy OP28](#)).
2. The victim of a crime discloses PHI to a law enforcement person.
3. Disclosures are made during a complaint investigation.

Sample Situations: Sanctions

A physician who is the PI conducting a research study involving human subjects fails to follow the protocol to obtain written authorization for participation in the study. Upon routine review of the study, the failure was discovered. What is the appropriate sanction?

- The patients' privacy has been violated because their records were accessed without either their authorization or an alternative permitted under the Research Policy. For failure to comply with both the HIPAA regulations and the URM/Strong Health policy, this physician/PI is subject to sanctions. The Privacy Officer will confer with the Senior Associate Dean for Research to determine the proper disciplinary sanction which could include:
 1. Exclusion of the data not obtained with appropriate authorization
 2. Shutting down the study
 3. A possible penalty for the physician/PI
 4. Written notice with a copy to the Chair for inclusion in that physician/PI's file
 5. The physician/PI prepares an in-service for his/her department.

A nurse overhears that a neighbor has had a stillborn delivery. She grieves for the neighbor and as a friendly gesture, orders a fruit basket to be delivered to the family, who didn't want to share this experience with anyone. Has the patient's privacy been violated, and if so, what is the appropriate sanction?

- Yes, the patient's privacy has been violated, even though the nurse was well intended (the family obviously wanted to keep this as private as possible). This nurse is subject to disciplinary sanctions, which may include termination. The Privacy Officer will coordinate with Human Resources and the nursing director on the sanction.

An individual who takes trash containing PHI from a clinical area to the secure designated service collection point left the trash unattended while returning for the forgotten key. No one accessed the bins while the individual was gone, but the supervisor happened to walk by and notice the bins were unattended. Is this a privacy violation, and if so, what is the appropriate sanction?

- Even though patient information was not actually accessed, this could have been a violation of patient privacy. An appropriate sanction would be counseling and perhaps a review of job-specific training regarding the proper disposal of trash.

URMC/Strong Health HIPAA Privacy Training Module



POLICY SUMMARY: OP8

(for full policy, refer to <http://intranet.URMC.Rochester.Edu/Policy/HIPAA>)

Complaint Process

The HIPAA Privacy Rule provides for filing a privacy-related complaint. As much as possible, complaints should be dealt with and resolved at the point of origin through normal channels. However, at any time, an individual may file a HIPAA privacy complaint either to the appropriate URMC/Strong Health Privacy Officer or to the Secretary of Health and Human Services. Individuals are provided with information concerning their right to file a privacy-related complaint in the URMC/Strong Health Notice of Privacy Practices.

URMC/Strong Health will review privacy-related complaints and respond to the individual, as appropriate.

Who needs to follow this policy?

Anyone who receives a privacy-related complaint.

What type of complaint might a patient or family member have regarding PHI?

A patient may:

- Feel they have been denied access to their PHI.
- Disagree with a denial to amend a medical record.
- See a violation of the URMC/Strong Health Notice of Privacy Practices.
- Feel there is a violation of the Privacy Rule.

What is the complaint process?

When a patient or family member speaks to a staff member about a privacy complaint, the normal problem solving process should be followed to attempt to resolve the problem.

Privacy-related complaints could also be directed to the Privacy Officer (see [Policy OP4](#)). Once the Privacy Officer has received the complaint, they will document it, review it and determine steps for resolution.

If a staff member wishes to report a privacy complaint anonymously, they can call the University/Strong Health Integrity Hotline at 756-8888.

What if the patient or family member does not want to speak to the Privacy Officer, or asks for outside help?

Anyone can contact the Secretary of Health and Human Services with a privacy complaint. If a staff member becomes aware that a patient expresses intent to file this type of complaint, the staff member should notify the Privacy Officer immediately.

Once a patient or family member has filed a complaint, what action can URM/Strong Health take against them?

None. The patient or family member has a right to file a complaint, participate in an investigation of a complaint, testify at a hearing or assist in a compliance review without interference or retaliation.

Sample Situations: Complaint Process

As a social worker walks by two nurses speaking about a patient's diagnosis in the cafeteria, she also overhears the patient's name. She does not know these nurses, but is pretty sure they are in violation of the HIPAA privacy rules. What should she do?

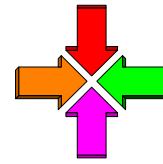
- She can remind the nurses that under the law, we need to ensure that a patient's PHI is not discussed in an open area. If she does not feel comfortable doing this, she should talk to the nurses' supervisor or call the University/Strong Health Integrity Hotline at 585-756-8888.

Sue is upset because her health care treatment was disclosed to a family member without her knowledge. She is on the phone and angrily demanding to speak to "someone in charge." What do you do?

- Ask her if she would be willing to give you some information that you can relay to your manager. Speak to your manager immediately so that s/he can consult with the Privacy Officer for resolution.

Frances is in the middle of her weekly home visit when the nurse begins to tell her about another patient who is having similar therapy and how much better Frances is doing than the other patient. Although a name was not used, Frances does not feel right hearing this information. Has a privacy violation occurred? If so, what can Frances do?

- A privacy violation has not occurred, since the nurse did not reveal any personal information about the other patient. However, Frances can tell her nurse that she would rather not hear anything about other patients.



URMC/Strong Health HIPAA Privacy Training Module

POLICY SUMMARY: OP14

(for full policy and related procedure, refer to <http://intranet.URMC.Rochester.Edu/Policy/HIPAA>)

Minimum Necessary Information

When using, requesting, or disclosing protected health information (PHI), URMC/Strong Health will use reasonable efforts to restrict access to PHI to the minimum necessary to accomplish the purpose for which the information is being used, disclosed or requested.

Who needs to follow this policy?

Any member of the URMC/Strong Health workforce who has access to PHI, needs to review PHI to perform their role, or disclose PHI to another person or agency.

How does a workforce member determine what is appropriate use and disclosure of PHI when someone requests release from them?

There are three types of situations to consider:

1. Using or disclosing PHI without the need to determine if the minimum necessary rule applies.
2. Relying upon another person's determination that the request is reasonable and is for the minimum necessary information to do the job.
3. Releasing PHI once it has been determined by the workforce member that the request is reasonable and appropriate.

Under what circumstances would information be released without needing to determine whether or not the information is the minimum necessary?

When:

1. Healthcare providers treat patients.
2. A patient, or their healthcare representative, requests PHI.
3. An authorization describes the PHI to be released.
4. The Department of Health and Human Services requests PHI.
5. The law *requires* use or disclosure of PHI.
6. The disclosure is for standardized transactions (for example, billing).
7. Another covered entity requests it and the request is reasonable.
8. A researcher has IRB (Institutional Review Board) or Privacy Board approval, and the request is reasonable.

Under what circumstances would a member of the workforce rely on another person's determination that a request for information is reasonable and the minimum necessary?

1. When URMC/Strong Health is disclosing information to a public health official to report or prevent disease, injury or child abuse or neglect.
2. When URMC/Strong Health is disclosing information to a public health official to report births, deaths or other vital events.
3. When a URMC/Strong Health business associate requests information to provide professional services to URMC/Strong Health.

In all other circumstances, URMC/Strong Health must follow these rules when using or disclosing PHI:

1. Determine which workforce members need access to PHI and what categories of PHI to do their jobs.
2. Limit access by workforce members to those categories of PHI that are reasonably necessary to do their job.
3. Develop and implement procedures or protocols for routine requests for PHI that limit the information disclosed to the amount that is reasonably needed to meet the request.
4. Evaluate nonroutine requests for PHI on a case-by-case basis, considering (a) the purpose for the request, (b) whether or not the release is permitted under URMC/Strong Health policy, (c) the kind of PHI that is necessary to meet the request and (d) whether or not the request could be met by using a lesser amount of PHI.
5. Consider the cost, operational burden and impact to patient care of any limitations when determining how much information to release.

What does each member of the URMC/Strong Health workforce need to consider when asking for PHI to be released to him or her?

It is each individual's responsibility to limit his or her requests for uses and disclosures of PHI to the minimum necessary to accomplish their task.

Note: An entire medical record should not be requested or disclosed unless it is reasonably necessary to accomplish the work, or it is not practical to pull the record apart before releasing it to the requestor.

The only exception is when the request is for treatment—minimum necessary does not apply in those cases.

Sample Situations: Minimum Necessary

A housekeeper on the pediatric floor asks the Nurse Manager why one of her favorite patients was discharged so soon after surgery. What can the Nurse Manager tell the housekeeper?

- The housekeeper does not need any medical information to perform her role; the Nurse Manager can only tell her that the child was discharged.

A Social Worker is counseling a family on living assistance for their elderly parent who is being discharged tomorrow. What PHI can the Social Worker have access to while discussing arrangements with the family?

- In order for the Social Worker to assist in appropriate discharge plans, he/she may need further understanding of the patient's ability prior to hospitalization, hospital course (for example, complications), and prognosis. Additionally, they will need detailed financial information in order to assist the patient and the family in making the appropriate choices. (For example, is discharge to home reasonable or will the patient require a skilled nursing or assisted living facility?)

An ambulance delivered a critical patient to the ER last week and did not get a chance to ask for demographic information. The company has called the hospital and is asking for the patient's name, address, etc., for insurance information for billing. Can this information be released?

- Yes, this is a routine disclosure for payment.

A Dental Hygienist is new to the office and would like to prepare for his first day with his new patients. What information can he access to provide the best patient care?

- He can have full access to records of those patients he will be working with directly. He cannot, however, have access to patients who are not his.

An Ambulatory Patient Rep (APR) schedules patients as part of her job responsibilities. While on the phone confirming his next appointment, a patient tells her that he has not received a bill for his last office visit. Can the APR access his information?

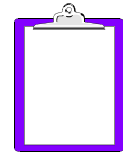
- Yes, she can access a summary of the billing information (demographics) to determine if his address is correct. She cannot discuss details of payments and needs to transfer the call to a billing clerk if the patient wants more specific information.

Information Systems is running a report for the Cardiovascular Department to include all patients who have had heart surgery in the past 18 months who have had no post-surgical complications. What kind of information can they access?

- It is the responsibility of the workforce member running the report to ensure that the individual requesting the report is authorized to have access to the information and that only the minimum necessary specific information is released for that report.

A Physical Therapist specializes in working with patients who have arthritis. What information does that therapist need while working with each patient?

- The therapist has access to all medical records to ensure she has a complete picture of the patient's health, but it is her responsibility to view only information that is relevant to the patient's current condition.



URMC/Strong Health HIPAA Privacy Training Module

POLICY SUMMARY: OP19

(for full policy, refer to <http://intranet.URMC.Rochester.Edu/Policy/HIPAA>)

Acknowledgement of Notice of Privacy Practices

URMC/Strong Health will make a good faith effort to provide individuals with the Notice of Privacy Practices at the time of the first service delivery after April 14, 2003. If the first service delivery after that date is an emergency treatment, the Notice will be provided as soon as practicable after the emergency treatment situation.

Who needs to follow this policy?

Anyone who provides services to patients who may be the patient's first contact with the healthcare organization.

What is the Notice of Privacy Practices?

It is URMC/Strong Health's notice to patients that contains a complete and detailed description of the possible uses and disclosure of PHI, as well as certain patient rights.

How does a patient acknowledge they have received the Notice?

The patient is asked to sign a receipt when they receive the Notice, which will become part of that patient's medical/administrative records related to the service provided.

Can patients refuse to sign for the Notice?

Patients should be encouraged to sign once the Notice has been received, but if they are unwilling or unable, the health care provider must document that efforts were made to acquire a signature and why that signature was not received. That documentation becomes part of the patient's records.

What does the patient do if she/he does not understand or has questions regarding the Notice?

The patient should make their concerns/questions known to their healthcare provider.

Sample Situations: Acknowledgement of Notice of Privacy Practices

Dr. G's patient is returning for her routine allergy shot; does she need to acknowledge the Notice of Privacy Practice each time she comes in to the office?

- No; once a Notice has been signed after April 14, 2003, that Notice is sufficient.

The police bring a man into the ED who is high on drugs and not very coherent; should he be asked to acknowledge a Notice of Privacy Practice?

- The man's signature merely acknowledges that he has received the Notice, not that he has read it, agreed with it, or understood it. If the healthcare provider believes that it is not appropriate to provide at the time of registration, the registration rep should make a notation on the form that the signature was not obtained. If it is felt that in the patient's state, he is able to accept the Notice and sign that it was received, that is permissible.

A Home-Health Aide has been given two new patients this week. Does the Aide need to provide a Notice of Privacy Practice to her new patients?

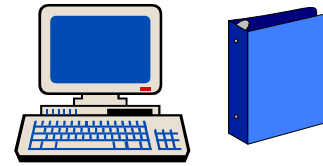
- The VNS nurse that opens the case will obtain the signature that the patient has received the Notice; therefore, the Aide does not have to obtain a signature.

A woman is brought into the ED following an automobile accident. She is a "Blue 100" with severe injuries and no family present. What should the registration rep do regarding the Notice Acknowledgment?

- In an emergency situation, it is not necessary to provide the Notice and obtain a signature until, or if, practicable after the emergency treatment situation.

A patient at the SON flu shot clinic refuses to sign an Acknowledgement of Notice of Privacy Practices. What should the registration clerk do?

- The patient will receive the flu shot; the registration clerk makes a note on the form noting that the patient declined to sign.



POLICY SUMMARY: 0P23.1

(for full policy, refer to <http://intranet.URMC.Rochester.Edu/Policy/HIPAA>)

Uses and Disclosures for Facility Directory

A health care facility is allowed, but not required, to use or disclose protected health information (specified below) about an individual for a facility directory provided the individual is informed:

- That the protected health information may be included in patient directories.
- Who may have access to directory information.
- How they may restrict or prohibit some or all of the permitted facility directory uses or disclosures as described below.

Who needs to follow this policy?

Anyone who has personal, paper or electronic access to a patient's PHI (**P**rotected **H**ealth **I**nformation) such as their name, location, general condition or religion.

What is a facility directory?

Any listing of active patients, either on paper or electronically, that contains a patient's name, condition, location and religious affiliation.

Are all active patients listed in the facility directory?

No; patients can decide if they do not want to be included in the directory and can make their wishes known orally to nurses, doctors, admission personnel or other appropriate medical facility staff. Patients are given a meaningful opportunity to discuss their wishes while they are being treated or admitted.

If a patient wants to be included in the facility directory, do they have to give all of their personal information?

No; patients can choose *not* to include their religion as part of the directory information.

What if a patient cannot tell a hospital staff member their wishes about being in the directory while they are being treated or admitted?

Providers/staff need to decide, based on the patient's best interest, whether or not it is necessary to include *some* information (name, for example) in a directory until the patient can make a decision.

If a patient is listed in the facility directory, who can ask for their information?

Family members, friends, clergy, etc., can ask about a patient **by using their full name.**

Examples:

- “Marion Jackman was brought in through emergency; how is she?”
- “What floor is Henry Rees on? I have a flower delivery.”
- “I’m here to pick up Kathleen O’Grady; where is she located?”

What kind of information will be given about the patient?

The patient’s location and general information regarding their condition can be given to the person who asks, *if that patient is in the directory.* Staff can say:

- “She’s been brought to 6-1400 and is in satisfactory condition.”
- “Mr. Rees is located on 5-1200.”
- “Kathleen is on East-7.”

What will friends and family be told if the person is not in the directory?

“I’m sorry, I don’t have any information available on a patient by that name.”

Is there anyone who can ask about patients without using the full name?

Yes, members of the clergy who have an ID badge from Chaplaincy Services can be given the names of the members of their congregation along with the patient’s condition and location, but *not* be given specific details about their illness or treatment.

Sample Situations: Uses and Disclosures for Facility Directory

A hysterical woman calls the hospital front desk and asks about her recently married niece who she heard was brought in an hour ago. The woman cannot remember her niece’s new married name because she is so distraught. What information can be given to this woman?

- None. The front desk receptionist needs to explain that no information can be released without the caller using a full name. If the woman eventually remembers her niece’s name, she can call back and will be given a one-word description of the niece’s condition. The Information Desk could suggest that the woman call another family member.

Reverend Anderson, the pastor of an Episcopal Church asks to see the listing of the patients from his congregation. He has a hospital identification badge from Chaplaincy Services indicating he has been identified as a member of the clergy. What can he be told?

- He may see a listing of the members of his congregation containing the patient names, their location in the hospital, and a one-word condition description.

An unconscious man is brought into Emergency by ambulance. His condition is so serious that he needs immediate surgery to save his life. There is no one with him to verify whether or not he should be listed in the facility directory. What should the hospital do in this case?

- The health care provider makes a decision based on his/her best judgment. Once a personal representative has been identified, he or she may be asked about the patient's wishes, or after the emergency situation has been resolved, the man can be asked about his preference.

A news reporter comes to the hospital Information Desk and asks, "How's that woman doing that was involved in the bad car accident on the expressway this morning? I heard she was brought here." What information can he be given?

- None; the news reporter is not given information because he did not ask for the woman by name. However, if the reporter asks about the woman using her name, he can be told a one-word description of her condition.

During the admission process, the staff member registering Mr. J informs the patient that the hospital maintains a directory, explaining that the information in the directory includes name, general condition, location and religious affiliation. Mr. J is asked whether he wants to be listed in the directory. Mr. J tells the registrar that he does not think he wants to be included. What should the registrar say to him?

- It should be explained to Mr. J that by not being in the directory, the hospital would be unable to acknowledge his presence should anyone call about him or ask for him at the Information Desk. Mr. J decides that he would like to receive visitors and deliveries and therefore tells the staff member that he wants to be included in the directory after all.



URMC/Strong Health HIPAA Privacy Training Module

POLICY SUMMARY: 0P25

Uses or Disclosures of PHI for Research Activities

(for full policy and related procedures, refer to <http://intranet.urmc-sh.rochester.edu/Policy/HIPAA>)

Scope

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) outlines the conditions under which a covered entity may use or disclose health information for research purposes. This policy applies to all research involving human beings or materials from human beings, including records or information from individuals, alive or deceased, regardless of sponsorship or whether regulated by the Food and Drug Administration.

Policy

Protected health information (PHI) may not be used internally or disclosed to any persons or organizations outside The University of Rochester Medical Center/Strong Health (URMC/SH) covered entity for research purposes, regardless of the source of funding, except in accordance with this policy.

As a general rule, in order to conduct research using PHI, **one** of the following conditions must be met:

- *The researcher must obtain the research subject's authorization; or
- *The Research Subjects Review Board (RSRB) or the URMC/SH Privacy Board must approve a waiver of the individual authorization; or
- *The PHI must be de-identified (as defined in HIPAA Policy 0P30 De-identification of PHI); or
- *The PHI must be part of a limited data set and a data use agreement must be signed and on file; or
- For reviews preparatory to research, appropriate representations about the research must be provided by the researcher to the data manager of the requested records.
- For research on a deceased person, appropriate representations and documentation must be provided by the researcher.

*indicates RSRB involvement

The specific requirements for each of these conditions are discussed below.

Special expanded rules and modification of the standard research authorization language apply to the use and/or disclosure for research purposes of **any** of the following types of information:

- HIV-related information
- Alcohol and substance abuse information
- Mental health information

- Genetic tests and results from genetic tests

Additional information can be found in the procedures at the end of the complete policy document or contact the Research Subjects Review Board or the Research HIPAA Privacy Officer for help with specific questions.

All research activities must also comply with other applicable University and URM/SH entity policies relating to research such as policies addressing FDA requirements for research, use of the minimum amount of PHI necessary to conduct the research (URM/SH [Policy 0P14, Minimum Necessary](#)) and with any additional requirements that apply to the specific type of information identified above as having special rules. Finally, to the extent medical and healthcare staff provide treatment to subjects as part of a research study, they must follow the appropriate procedures of their URM/SH entity.

For complete information regarding this policy, see the Procedures Section of this policy at <http://intranet.urmc-sh.rochester.edu/policy/HIPAA/Privacy/P25.pdf> . Any questions about this policy should be directed to the Research Privacy Officer. For name and address/number see <http://intranet.urmc-sh.rochester.edu/policy/HIPAA/FAQsResources/Officers.asp#Security>

Who needs to follow this policy?

Any member of the workforce who engages in research or clinical trial activities involving specimens, records or information from human beings, or in administrative activities in support of those activities.

What is considered research under this policy?

Any systematic investigation (including development, testing and evaluation) that has, as its primary purpose, the development of or contribution to generalizable knowledge. This includes the development of research repositories and databases for research. Research also includes any experimental use of a drug or device that is regulated by the Food and Drug Administration (FDA).

Case Studies are reports of treatment and are not generally considered research; however, certain activities associated with case studies would be considered research and require that those activities comply with this policy and its procedures (see Section 12 of the Procedures Section of [Policy 0P25](#)).

Note: quality assurance and utilization management are not governed by this policy.

What is the definition of primary purpose under this policy?

The primary purpose of the investigation must be the development or contribution to generalizable knowledge. If, however, the primary purpose changes as results are analyzed, and those results are generalizable, the researcher must document the change in status by notifying the IRB and complying with the IRB's review process.

What are the definitions of use and disclosure under this policy?

Use - Information that is shared within the URM/Strong Health covered entity, and is under direct control of URM/Strong Health, has been used.

- For example, a clinical trial coordinator in the School of Medicine and Dentistry who is analyzing a research subject's individually identifiable health information is **using** PHI.

- Disclosure - PHI that is shared with someone who is not an employee, student, volunteer or otherwise under the direction and control of the URM/SH covered entity, has been disclosed.
- For example, showing source documentation which includes PHI to a clinical trial sponsor's representative is a disclosure, even if the representative does not remove the PHI from the URM/SH research site.

Authorization

A patient/research subject's permission must be obtained before using their PHI for most research. A separate authorization may be used. However, in most cases, URM/SH combines the research authorization with the 'informed consent' document required for human subjects research. Authorizations must contain certain elements and statements in order to be HIPAA compliant. They include such items as the information you intend to use, people/ organizations who may use or disclose the information, people/organizations who will receive the information, and the right of the patient to revoke the authorization. Standard wording for an authorization can be found on the RSRB website:

<http://www.urmc.rochester.edu/rsrb/rsrbforms.htm>

Note that research involving information from the following areas requires specific authorization language which differs from the standard authorization language:

- HIV Information
- Mental Health
- Alcohol and Substance Abuse
- Genetic Information

Consult the procedures section of [Policy OP25](#) for additional guidance for these areas.

Waiver of Authorization

In some cases, such as to conduct records research, it may not be practicable to obtain a research subject's signed authorization. PHI may still be used for research if the RSRB or the Privacy Board approves a waiver or partial waiver of authorization. Most requests for waiver of authorization require RSRB review. In some cases, where RSRB approval is not required and filing for an exemption with the RSRB is not required, the Privacy Board would review the request. More detailed information on the waiver process is available from each Board.

Reviews Preparatory to Research

Use and disclosure of PHI for reviews preparatory to research may be permitted without an authorization; for example to design a research study, assess the feasibility of a study or to aid in recruitment of study subjects. The researcher must provide the data manager of the records from which the information will be taken a written certification indicating the records need to be reviewed for preparatory to research activities, no PHI will be removed from URM/SH, and that the PHI sought is necessary for research purposes.

Research on Decedents Information

Use of decedent PHI is permitted if the researcher provides written representation to the data manager that only decedent information is sought and the information is necessary for research purposes. The researcher must also agree to provide documentation of the death of the individuals being studied, if requested to do so by the Privacy Board. Disclosure of decedent research information requires the authorization of the executor/administrator of the decedent's estate unless a waiver of authorization has been approved, the PHI has been de-identified, or is a part of a limited data set.

De-identification

There are specific requirements that must be met in order for information to be considered de-identified. Once de-identified, information can be used for research purposes subject to the provisions of URM/SH Policy 0P30 De-identification of PHI at:

<http://intranet.urmc-sh.rochester.edu/policy/HIPAA/Privacy/P30.pdf>

Limited Data Set and Data Use Agreement

A researcher may use or disclose information in a limited data set without authorization from a research subject if certain specific conditions are met. The limited data set must exclude direct identifiers **except** town, city, state, zip code, all dates relating to an individual, and unique codes or identifiers not listed as direct identifiers. The recipient of the limited data set must also sign a data use agreement.

Disclosures to the Food and Drug Administration — Minimum Necessary

PHI disclosures may be made to the FDA subject to certain conditions outlined in [Policy 0P24.2](#), Disclosures for Public Health and Health Oversight Activities, as well as [Policy 0P14](#), Minimum Necessary.

Accounting of Disclosures

The Privacy Rule gives individuals the right to receive an accounting of certain disclosures; the accounting must include disclosures of PHI that occurred after April 14, 2003, or for the six years previous to their request (whichever is sooner). The accounting must include specific information regarding each disclosure, except when the disclosure:

- was made in accordance with or after receiving individual authorization
- was part of a limited data set with a data use agreement, or
- was de-identified information.

Researchers must keep records of disclosures of PHI when the disclosure was:

- made under a waiver of authorization, or
- made in connection with preparatory to research activities.

Disclosures are recorded in the Disclosure Application Log at:

<http://intranet.urmc-sh.rochester.edu/policy/HIPAA>

The HIM Department or the Office Manager in a faculty practice is responsible for responding to requests from research subjects and patients for accounting of disclosures. For additional information, see Policy 0P9, Accounting for Disclosures:

<http://intranet.urmc-sh.rochester.edu/policy/HIPAA/Privacy/P9.pdf>

Health Services Research

Health Services research is designed to improve the quality of health care, reduce costs, improve patient safety, decrease medical errors and broaden access to essential services, helping health care decision makers make more informed decisions. These studies are carried out by analyzing large databases of health care information, and the principle risk to participants is not physical harm, but loss of privacy. If a covered entity undertakes a study that instead of understanding and improving its own service, results in obtaining generalizable knowledge, then it is considered a research study and not a health care operations activity. Health services researchers must submit all research study protocols to the RSRB for review; the Board will determine which, if any, sections of the Human Subject Protection rules and the Privacy Rule apply to the specific protocol.

The Privacy Rule does permit a covered entity to gather information on patients for treatment, payment, and health care operations and put this information in their own database for these purposes without Authorization. Covered entities are also permitted to disclose PHI without Authorization to government-authorized public health authorities for disease surveillance and prevention and other public health purposes.

Research Databases and Research Repositories

Research databases and repositories containing PHI and created exclusively for current or future research purposes are subject to the terms and conditions of this policy and require RSRB approval for:

- the creation of the database,
- the process of adding PHI to the database, and
- the use of the database for research.

Exceptions to this approval process include if the researcher has obtained:

- a Consent/HIPAA Authorization from the subject,
- a Letter of Exemption from the RSRB for the use of PHI,
- an RSRB-approved Informed Consent prior to 4/14/03, or
- an Express Legal Permission prior to 4/14/03 that was not study-specific and authorized future unspecified research.

The Privacy Board must review databases, repositories, and registers containing decedent information; the approval submittal form is located at:

<http://intranet.urmc-sh.rochester.edu/policy/HIPAA/Research.asp>.

Procedures for submitting research protocols to the RSRB are located at:

<http://www.urmc.rochester.edu/rsrb/FORMS.HTM>

If the scope of the originally approved database or repository occurs, Privacy Board or RSRB approval must be obtained again.

Case Studies

A case study is a report of treatment (including innovative treatment; for example, surgery) and, as such, does not meet the Common Rule definition of research (a systematic investigation, including research development, testing and evaluation designed to develop or contribute to generalizable knowledge). Case studies that contain identifiers will be reviewed by the Privacy Board, where any need for authorization will be determined. Case studies that

contain no PHI with identifiers do not need to be reviewed by either the Privacy Board or the RSRB, but note that a unique condition itself may be considered identifiable.

However, if any of a number of conditions are present, the activity may be considered research rather than a case study. These conditions include: plans to offer the treatment to some individuals but not others; investigational drugs or devices; collection of data that would not usually be collected during clinical practice; an attempt to manipulate treatments to test if they work consistently well; if there is a protocol or study plan; if separate sets of records or data are maintained, particularly with identifiers; if the primary purpose is to answer a research question and not for providing clinical care; or there is consideration that the treatment may yield a case series. Check with RSRB or the Research Privacy Officer to determine whether your particular situation is a case study or research.

Sample Situations: Uses or Disclosures of PHI for Research Activities

Dr. D is a self-employed community physician conducting an independent IRB-approved study of a new drug that is being given to a select group of surgery patients while they are in a Strong Health hospital. With appropriate approval, he is pre-screening potential participants by reviewing the previous day's surgical admissions logs as part of a review preparatory to research; URM/Strong Health staff must keep track of this in the Disclosure Log. If asked, does the hospital need to provide an accounting to patients, telling them that their PHI was reviewed, even if they did not become part of the study?

- Since Dr. D is **not** employed by URM/Strong Health, pre-screening patient PHI is considered a **disclosure** for research purposes. If a patient requests an accounting of disclosures of PHI, the patient must be provided with an accounting of the disclosure, regardless of whether or not they were seen by Dr. D in his office or became participants in the study. URM/SH staff who provide Dr. D access to the PHI must make sure the Disclosure Log is completed.

If Dr. D had been **employed** by URM/Strong Health, the prescreening reviews of the logs would have been considered a **use** and not subject to an accounting.

Ms. J, a clinical coordinator for a URM department, is also looking at the previous day's surgical admissions logs as part of a review preparatory to research. The trial sponsor, Acme Drug Company, sends a monitor who has asked to review the admissions logs as well. Is this allowed under HIPAA regulations?

- No; monitor reviews are not considered preparatory to research. HIPAA allows disclosures when a researcher is completing reviews preparatory to research.
- The monitor could see information pertaining to subjects who were enrolled in the study, but not information about prospective participants.

The information could be provided to the monitor as de-identified information.

Dr. O, a full-time faculty member, has enrolled subjects in a clinical trial for a new asthma drug. A subject withdraws from the trial, providing a written notice. Dr. O sends a partially completed case report form to the trial's sponsor. Was this an appropriate action for Dr. O to take?

- If it was necessary to preserve the integrity of the trial, Dr. O could have sent the form to the sponsor. However, HIPAA prohibits using or disclosing additional information after a subject's written withdrawal.

An elderly man participating in a drug trial suddenly dies. The attending physician, a full-time faculty member, believes the trial drug probably caused or contributed to the man's death. The physician in charge of the study contacts the RSRB chair who contacts the URMCMC Office of Counsel attorney to discuss how to handle the situation. May PHI be disclosed to:

- The OCMC attorney? Yes, since this information is related to health care operations, sharing of the information inside the covered entity is considered a **use**.
- The trial sponsor? Yes, if authorization or waiver of authorization allowed for the reporting of case-based events.
- The FDA or Office for Human Research Protection? Yes, since this would be considered a public policy disclosure which is permitted for health oversight activities.
- The director of the hospital to conduct a quality assurance investigation? Yes, this is considered a part of hospital operations.
- The press? No, unless an authorization has been obtained from the subject prior to participating in the clinical trial, this information cannot be released.

Professor C, a full-time faculty member in a University of Rochester River Campus department that is not part of the URMCMC/Strong Health covered entity, wishes to obtain PHI for purposes of a research project. What options does Professor C have to obtain this information?

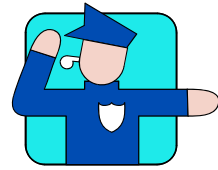
- Since the project involves human subjects, Professor C must follow the RSRB process for study review and approval.

Use of PHI for research purposes in the project is subject to the same rules as specified in [Policy OP25](#) including meeting one of the following conditions (Note that since Professor C is not part of the URMCMC/SH covered entity, PHI is being disclosed as opposed to being used):

- obtaining the research subject's authorization;
- obtaining an IRB or Privacy Board waiver of authorization and completing the disclosure log;
- complying with the reviews preparatory to research conditions;
- obtaining authorization from the administrator or executor of the decedent's estate for research on a decedent's information, since this would be a disclosure of PHI;
- using de-identified information; or
- using a limited data set and signing a data use agreement.

Dr. H has received RSRB approval for a research study. The study protocol includes obtaining authorization from study participants using a HIPAA-compliant authorization. While taking a medical history of a study participant (who had signed a HIPAA-compliant authorization) Dr. H learns the study participant was diagnosed with HIV. Can Dr. H use this information in the study?

- In this case, the original HIPAA-compliant authorization is not sufficient to allow Dr. H to use the HIV information in the study. Dr. H must obtain another authorization from the study participant that is HIV/HIPAA-compliant before using or disclosing the HIV information as part of the study. HIV-compliant authorizations can be obtained from the following sources:
 - New York State HIPAA-Compliant Authorization for the Release of Medical Information and Confidential HIV Information (Form DOH 2557). The Form can be obtained from the NYS DOH website:
<http://www.health.state.ny.us/forms/doh-2557.pdf>
 - SH Form 2557, which is HIPAA/NYS-compliant, may also be used. This form is available through the Forms Management department.



URMC/Strong Health HIPAA Privacy Training Module

POLICY SUMMARY: OP28

(for full policy, refer to <http://intranet.URMC.Rochester.Edu/Policy/HIPAA>)

Disclosures by Whistleblowers and Workforce Member Crime Victims

The HIPAA privacy regulations safeguard covered entities from action for disclosures made by whistleblowers as part of the reporting of a violation. In certain situations, a URMC/Strong Health workforce member may disclose protected health information (PHI) to a health oversight agency or to an attorney, and such disclosures are not treated as a violation of the regulations. Also, a URMC/Strong Health workforce member who is a victim of a crime may disclose identifying PHI about the suspected perpetrator to a law enforcement official, and such disclosure is not considered to be a violation of the regulations.

Who needs to follow this policy?

Any member of the URMC/Strong Health workforce (staff/faculty/volunteers/students) who needs to disclose PHI as a whistleblower or is the victim of a crime.

What is a whistleblower?

Any member of the URMC/Strong Health workforce who in good faith reports what is thought to be wrongdoing within the organization.

What kind of violation would be reported by a whistleblower? Some examples might include:

- Any unsafe practice that could cause harm to a patient, workforce member or the public
- Suspected fraud or abuse
- Privacy violation

Who would the workforce member call to report a violation?

Workforce members are always encouraged to report any concerns to their supervisor. Concerns can also be reported anonymously to the Privacy Officer or the Strong Health Integrity Hotline at 756-8888. Disclosures may also be reported to:

- Any public health agency that has the authority to investigate URMC/Strong Health entities,
- A lawyer who the workforce member has hired to help them look into the situation, or
- JCAHO or other accreditation organization

Victim of a crime

If a member of the workforce is a victim of a crime, they can disclose PHI to the police or other law enforcement officials as long as the information is about the person suspected of committing the crime.

What PHI can be released?

Only the following:

- Name and address
- Date and place of birth
- Social security number
- Blood type and rh factor
- Type of injury the suspect may have
- Date and time of treatment
- Date and time of death, if applicable
- Description that includes height, weight, eye color, race, etc.

Are there exceptions to this?

Yes, URMC/Strong Health cannot disclose information about DNA or DNA analysis, dental records or typing, samples or analysis of body fluids or tissue.

Sample Situation: Disclosures by Whistleblowers and Workforce Member Crime Victims

Sam W. was brought into the ED complaining of severe stomach pain. When he was told he could not have Demerol for the pain, he became violent and lunged at the attending physician, knocking him to the floor before storming out the door. The police were notified of the incident by the facility's Security Department. When the police arrived, they asked the attending physician for information on the assailant. What information can the attending physician give?

- The attending physician can relate the following information: that Sam W. is a white male, about 6 feet tall, weighing 250 pounds, with black hair and beard and a tattoo of an eagle on his upper right forearm. If his address is known, it can also be released.

The attending cannot release Sam's HIV status, DNA, dental records or analysis of blood or body tissue.