Roswell Park Cancer Institute Policy and Procedure	**Date Issued:** 2/1/1987	**Number:** 408.10
Title: Confidentiality Of Health-Related Information	**Revision No:** 15	**Effective Date:** 5/4/15
Prepared by: Director, Health Information/ Medical Record Department; General Counsel	**Approved by:** Michael B. Sexton, General Counsel	**Page:** 1 of 8

A. GENERAL STATEMENT OF POLICY

Regulations issued under the federal Health Insurance Portability and Accountability Act (HIPAA) and New York State laws mandate securing the privacy and confidentiality of each patient's health information, including information in the medical record (paper or electronic). Information contained in a patient medical record is confidential and cannot be released to individuals without proper authorization of the patient, a subpoena or a court order, unless the release is covered under a regulatory exception. Medical records are the property of Roswell Park Cancer Institute (RPCI) and are maintained for the benefit of the patient, the medical staff, research purposes and the hospital. Medical records are stored in a fire protective secure area. RPCI is a covered entity and complies with HIPAA and New York law in protecting and maintaining the confidentiality of patient information, and prohibiting unauthorized or otherwise impermissible uses and disclosures of such information.

B. SCOPE

This policy and procedure applies to all personnel, students and volunteers of Roswell Park Cancer Institute and Health Research, Inc. Roswell Park Division and the Roswell Park Alliance Foundation (collectively "RPCI").

C. ADMINISTRATION

This policy and procedure will be administered by RPCI Administration, through the Health Information/Medical Records Director, the RPCI Privacy Officer, all Department Heads and Supervisors.

D. POLICY / PROCEDURE

1. Definitions:

    a. Protected Health Information: Information, including demographic information, that is collected from the patient, and is either created or received by RPCI and relates to the past, present or future physical or mental health condition of the patient, the provision of care or treatment to the patient, or the past, present or future payment for care or treatment of the patient, and which either identifies the patient or can be used to identify the patient, is called "Protected Health Information" or "PHI." There are legally requirements for the protection and maintenance of the privacy and confidentiality of PHI.

b. Minimum Necessary: Only the information that is needed for the immediate use or disclosure should be made available by the health care provider or other covered entity. This standard does not apply to uses and disclosures for treatment purposes (so as not to interfere with treatment) or to uses and disclosures that an individual has authorized, among other limited exceptions.

c. Treatment Purposes: The provision of health care by one or more health care providers, including by a health care provider with a third party. Treatment includes any consultation, referral or other exchanges of information to manage a patient's care. The Privacy Notice explains that the HIPAA Privacy Rule allows RPCI to use and disclose protected health information for treatment purposes without specific authorization.

d. Health Care Operations are certain administrative, financial, legal and quality improvement activities that are necessary to run RPCI and to support the core functions of treatment and payment. [45 CFR 164.501]

   Any of the following activities of the covered entity to the extent that the activities are related to covered functions: 1) conducting quality assessment and improvement activities, population-based activities, and related functions that do not include treatment; 2) reviewing the competence or qualifications of health care professionals, evaluating practitioner, provider, and health plan performance, conducting training programs where students learn to practice or improve their skills as health-care providers, training of non-healthcare professionals, accreditation, certification, licensing, or credentialing activities, 3) underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or benefits [Genetic information is a type of health information and it is not disclosable for underwriting purposes]; 4) conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs; 5) business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and 6) business management and general administrative activities of the entity. [45 CFR 164.501]

e. Payment Operations: Various activities of the health care providers to obtain payment or reimbursement for services provided. For a health care plan, activities to obtain premiums, to fulfill their coverage responsibilities, provide benefits under the plan and to obtain or provide reimbursements for care. Payment activities include the following:
   i. Determining eligibility or coverage under a plan and adjudicating claims
   ii. Risk adjustments
   iii. Billing and collection activities
   iv. Reviewing health care services for medical necessity coverage, justification of charges
   v. Utilization review activities
   vi. Disclosures to consumer reporting agencies (limited to specified identifying information about the individual, his/her payment history and identifying information about the covered entity)

f. Personal Representative: A person who has authority to make decisions related to health care on behalf of an individual who is an adult or an emancipated minor. This designation may occur when a patient is legally or otherwise incapable of exercising their rights, or when a patient simply chooses to designate another to act on their behalf with respect to these rights. Subject to certain exceptions, the Privacy Rule at 45 CFR 164.502(g) requires covered entities to treat an individual's personal representative as the individual with respect to uses and disclosures of the individual's protected health information, as well as the individual's rights under the Rule, including but not limited to access to the patient's PHI.

g. Qualified Person: A “qualified person” is a person either (i) authorized in writing by the patient to receive PHI, or (ii) having a valid reason to access the PHI for purposes of patient treatment or billing, or for necessary hospital operations.

2. Repositories of PHI

The medical record contains PHI, as do billing and registration records maintained by RPCI. PHI may also be located in paper or electronic records maintained in files, computer memory, databases, or other receptacles maintained in clinical, research or administrative locations. Any record, be it in paper or electronic format, containing PHI, shall be subject to this policy and procedure, as well as all other policies, procedures and rules of RPCI, and departments and mission areas endeavoring to govern confidentiality of and dissemination or disclosure of PHI.

3. Removal of Records from the Health Information/Medical Record Department or from the Hospital

Original medical records may be removed from RPCI’s jurisdiction and safekeeping only in accordance with a court order, subpoena, or statute. Medical records shall not be removed from the HIM Department except as necessary for the readmission of the patient, Medical Staff Committee meetings, or in the transaction of business of RPCI. Records that are removed from the HIM department are tracked, both by the person having custody of and the location of that record.

4. Telephone Requests

a. PHI may be given out over the phone only after verification of the caller's identity and verification that the caller is allowed access to the PHI requested.

b. Messages may be left on a patient's answering machine, such as for an appointment reminder. However, since the RPCI facility name implies a patient diagnosis, the facility name **must not** be used as part of the message.

5. Confidentiality

a. When using or disclosing PHI, RPCI makes reasonable efforts to limit PHI to the minimum necessary to accomplish the purpose of the use, disclosure or request. PHI, including information in the medical record concerning the condition of a patient, is confidential and should be discussed only to the minimum extent necessary to provide for the care and treatment of the patient. RPCI is responsible for preventing unauthorized access to or disclosure of a patient's confidential record/treatment from the time the medical record is initiated and during hospitalization as well as after.

b. Confidentiality Statement: All employees sign a confidentiality statement upon hiring at RPCI. This is kept on file in Human Resources.

6. Staff Access to Medical Records

An RPCI staff member/member of the workforce may only access medical records/information related to his/her job responsibilities. Access to medical records/information outside of job responsibilities, e.g. for family members, relatives, friends, etc., requires the patient’s written authorization. Staff members who are also RPCI patients, may not access their own medical record/information without either contacting Health Information Management and following the request process, or registering for MyRoswell and accessing via their MyRoswell login.

7. Requests for Health Information

   a. All requests for information from the medical record will be made to Health Information by a qualified person. All requests to obtain copies of medical records must be in writing and accompanied by an appropriate authorization. In specific situations, only the RPCI authorization may be used.

   b. Exceptions to this policy include the following departments who routinely send health-related information pertinent to their services according to their department policy. The departments include: Laboratory Medicine, Radiation Medicine, Pathology, Psychology, Employees' Clinic, Nuclear Medicine, Diagnostic Imaging, Clinical Genetics, Screening Clinic and Dental Department. An additional exception is the nursing supervisor acting in the absence of Health Information Medical Record personnel.

   c. Attorneys requesting to review records in the Health Information/Medical Record Department must submit a signed, written and dated authorization from a qualified person or a court order. The request, along with the patient authorization, must be sent to the Health Information/Medical Record Department prior to the review.

   d. Qualified persons shall receive no more than the minimum amount of PHI necessary to address the legitimate purpose to be served, or such greater amount as the patient has authorized in writing.

   e. Requests for the release of Mental Health and drug and alcohol abuse rehabilitation records – psychotherapy notes are not disclosable except with a patient's authorization and are kept separate from the patient's medical and billing records.

      i. PHI may be released without a patient's authorization if required by law:

         - To Public Health Authorities to prevent or control disease, injury or disability, and to government agencies authorized to receive reports of child abuse and neglect.
         - In limited circumstances to appropriate government authorities for victims of abuse, neglect or domestic violence;
         - In a judicial or administrative proceeding if the request is pursuant to a court order, subpoena, or other lawful process and disclosure of mental health records requires a court order in these proceedings in accordance with NYS MHY Sec. 33.13
         - Medical Examiner to determine cause of death.

      ii. Authorization

         All requests, including personal requests, should be forwarded to the Health Information/Medical Record Department for handling. All authorizations:

         - Must be in writing, but must not be dated prior to the period of hospitalization, unless the periods of hospitalization are related to previous visits.
         - Must specifically describe the PHI requested to be disclosed, must identify the entity authorized to make the disclosure (i.e. the RPCI Health Information/Medical Records Department), and the identity of the authorized recipient.
         - Must have the date upon which, or the event which will trigger, expiration or termination of the authorization, and a description of the procedure by which the authorization may be revoked. If there is no date specified, the authorization will expire one year after the patient signed the authorization. All authorizations will expire at the death of the patient

- Must be signed by the patient or the patient's personal representative, and the signature requirement is subject to the following:
    - If the patient is a minor (under age 18), the authorization must be signed by a parent or legal guardian.
    - If the minor's records pertain to treatment for history of abortion treated elsewhere, venereal disease, or if the minor is emancipated, the minor may sign the authorization to release records. An emancipated minor is any person who has married or is the parent of a child. A minor who is pregnant does not become emancipated until she gives birth.
    - If the patient has died, the authorization must be signed by the next of kin. If a legal representative has been appointed, a certificate from Surrogate's Court showing appointment of the representative shall be submitted. (When the spouse is also deceased and only children are surviving, the attorney should provide an Executor or Administration of Estate form from Surrogate court for release of medical records.)
    - Any requests for information from a medical record that contains HIV or AIDS related information should be forwarded to the Health Information/Medical Record Department. A special authorization form from the State must be completed and State mandates must be followed (see Policy No. 434.1).
    - If an inquiry is received from the news media about the condition of a patient, the caller shall be referred to the Communications Department (refer to Policy No. 408.8).
    - The signature on the authorization, should be preceded by statements indicating that (a) the patient understands that the PHI, once used or disclosed pursuant to the authorization, could be re-disclosed by the recipient and lose its confidential status; (b) that the authorized individual may inspect or copy the PHI to be used; (c) that the individual (patient or legal guardian) may refuse to sign the authorization; (d) that treatment, payment or enrollment may not be conditioned on authorization; and (e) if accurate, that RPCI will receive compensation in exchange for disclosing the information.

iii. Patient Access to Copies of Records:

- The patient may request electronic or hard copies of his or her PHI, including the medical record. The request must be in writing. The Health Information/ Medical Record Department must act on requests within 30 days. If the information cannot be gathered within the 30 day period, RPCI can obtain an one-time 30 day extension as long as the requestor is provided with written notice and provided with an expected date for receipt of the information. Access must be provided in the form requested, unless the form is not readily available. In that case, a readable hard copy must be produced unless the parties agree otherwise.
- The Health Information/Medical Record Department may provide a summary of the PHI instead of allowing the patient access, if the individual agrees and agrees to pay any fee charged for the summary.
- The Health Information/Medical Record Department will notify the attending physician involved in the patient's care that the request has been made. The attending physician must indicate an objection to the access within five days of the notification if he/she feels that the review would be detrimental to the patient or to another individual. If no objection is raised within 5 days, the HIM department will presume that he/she does not object. A denial of access is subject to appeal.

- If copies are made, the patient or his/her representative will be subject to the same fees for copying set forth for attorneys, insurance companies, etc. The fee is $.75 per page. Prepayment will be required for all copies.

iv. Patient Access to view medical record

The patient may request access to view their medical record. The Health Information/Medical Record Department will notify the attending physician involved in the patient's care that the request has been received. The attending physician shall indicate within five days of the notice that he/she feels that this review would be detrimental to the patient or to another individual, otherwise it will be presumed there is no objection to the access. A denial of access is subject to appeal. The HIM department has 10 days from the receipt of the request to provide the patient with access to view their medical record.

v. Patient Requesting "Immediate" Access to view medical record

In the event that an In-house patient is requesting urgent/expedited access to view their medical record, the staff member taking the request will notify the appropriate Clinician. The Clinician or their designee will meet with the patient as soon as possible, but within 24 hours, to review the record together.

8. Denial of PHI Access to a Patient or a "Qualified Person":

a. A physician may deny access to the following documentation.

i. Personal notes or observations
ii. Information disclosed to the provider under the condition that it be kept confidential.
iii. Information that the provider believes should not be disclosed regarding the treatment of a minor.
iv. Information that the provider believes will cause substantial harm to the patient or others.
v. Information obtained from other physicians who are still in practice. This information should be obtained directly from that physician
vi. Substance abuse records and clinical records of facilities licensed or operated by the Office of Mental Health. Mental hygiene law provides a separate process for the release of these records.

b. A denial must be timely, written in plain language, and must contain explanations of appeal rights and rights to complain to the Privacy Officer (including name, telephone) and to the Center for Medicare Services. On appeal, the licensed health care professional must respond within a reasonable period of time, and covered entity must notify the individual of the decision in writing.

c. In case of denial of access, a "qualified person" has the right to obtain a review by a licensed physician or nurse designated by RPCI to review such denials who did not participate in the original denial. The qualified person will be informed of his/her rights and given information as to how to pursue the review. If, following review, the reviewer determines that the PHI should be turned over to the subject, RPCI will comply. If the reviewer agrees with RPCI that the material should be denied, the qualified person may seek judicial review of that determination.

9. Accounting of Disclosure

Whenever RPCI discloses patient information to a third party, a copy of the subject's written authorization shall be added to the patient information or the names and addresses of the third

party and a notation of the purpose of the disclosure shall be indicated in the file or record. This also applies to governmental agencies for the purpose of inspections or professional conduct investigations. This does not apply to disclosures to practitioners or personnel employed by the hospital.

10. Patient Amendment/Challenge to Accuracy of the Medical Record

NY Public Health Law title 2, Section 18, NY Mental Hygiene Law Section 33.16(g) and 45 CFR §164.526 permit a qualified person (i.e. the patient) to challenge the accuracy of the information maintained within his/her medical record. A separate statement should be made disputing the information in question and to request an amendment. This request for amendment must be made a permanent part of the patient's medical record and be included with any future authorized disclosure(s).

Procedure:

a. Request for Amendment: A request for amendment is made by submitting the request in writing to the Health Information/Medical Record Department using the "Request for Record Amendment" form. (F 742). The Health Information/Medical Record Department shall act on the request within sixty (60) days after the date it receives the request. The Health Information/Medical Record Department may, on written notice to the requestor, extend this deadline by up to thirty (30) days. The Health Information/Medical Record Department shall investigate the request, including reviewing the request with the RPCI clinicians involved. After investigation, the Health Information/Medical Record Department shall either:

   i. Approve and Implement the Request. If approved, the requested amendment or change to the medical record shall be made, and the requestor shall be so notified. The Health Information/Medical Record Department shall modify the affected record by either changing the record itself or providing a notation and link on the record linking it to the amendment, which shall be appended to the affected record. The Health Information/Medical Record Department shall obtain from the requestor the name and address of each organization and individual that needs to be informed of the amendment. Any individual who had previously received the document that was amended will need to be informed of the amendment.

   ii. Denial. If the request is denied, the Health Information/Medical Record Department shall notify the requestor and provide an explanation of the basis for the denial. The requestor must be informed of their right to (a) submit a written statement of disagreement with the denial; (b) in lieu of a statement of disagreement, to request that the request for amendment and the denial be provided to any future recipients of a disclosure of the portion of the medical record that was the subject of the request; or (c) notify the Secretary of the Department of Health and Human Services, together with the address, name and title, and telephone number of the appropriate recipient of such complaint. If a statement of disagreement is submitted, the Department may submit a written rebuttal, and shall provide a copy of such rebuttal to the party who submitted the statement of disagreement.

   iii. Recordkeeping and Future Disclosures. The Health Information/ Medical Record Department shall, in the event of a denial, identify the information in the medical record that was the subject of the request, and append or otherwise link the request for amendment, the denial and any statement of disagreement or rebuttal filed. If a statement of disagreement has been filed, it, the request for amendment, the denial and any filed rebuttal, or an accurate summary of these documents, shall be included with subsequent disclosures of the information which was the subject of the request. If no statement of disagreement is filed, the requestor has the right to require that the

amendment request and denial be included in subsequent disclosures of such information.

b. Grounds for Denial of Amendment: A request for amendment may be denied where it is determined that the information or record sought to be amended or challenged:

   i. was not created by RPCI, unless the requestor provides evidence establishing that the original creator of the record is no longer available to act on the requested amendment;
   ii. is not part of the RPCI records;
   iii. is not subject to inspection by the patient or his or her representative; or,
   iv. is correct and complete in its original state.

11. Disposal Of Personal Health-Related Information:

    a. Scanned Records: After medical records are scanned, the paper record will be stored in the HIM department for 45 days. After 45 days, the paper will be destroyed following an appropriate quality assurance assessment. Exceptions are medical record documents of inpatients, ambulatory surgery patients and minor surgery patients which are stored for 2.5 years following the date of discharge or date of procedure, and shredded on site at RPCI.
    b. Microfiched Records: All medical records meeting the criteria for microfiching and destruction as specified by RPCI's record retention plan are transported to the contracted agency for this purpose. All medical records will be shredded upon receipt of a request for destroy order signed by the Director of Health Information/Medical Records or his/her designee. The medical record identification numbers of the charts destroyed are logged on the chart tracking system and the microfiche is filed in secure cabinets as a permanent record.

12. Breach of Confidentiality: Unauthorized access or use of health-related information (eg., patient record, computer data, employee health documentation) is a violation of federal law, Public Officers Law Section 74.3(c) and this policy. (Also see Policy 131.1 – Information/Data Breach)

13. Data Maintained in Hospital Information System: Confidentiality of patient and provider - specific information must not be compromised.

14. Access to data in the Hospital Information System and/or EMR is controlled via use of a security password and sign-on procedure established by RPCI's Information Technology Department.

15. No PHI or patient information should be left unattended in public areas.

16. Violations of this policy will be reviewed for disciplinary action, up to and including termination, in accordance with the procedures outlined in the collective bargaining agreements, if applicable.

E. DISTRIBUTION

This Policy and Procedure will be distributed to all RPCI Managers via the RPCI internal web page and to holders of backup hard copies of the manual. Managers are responsible for communicating policy content to pertinent staff.

F. REFERENCES

45 CFR Part 164.502 (b)(c)(d)