POLICY/GUIDELINE TITLE: Release of Protected Health Information (e.g., Medical Record) for Living Patients	ADMINISTRATIVE POLICY AND PROCEDURE MANUAL
POLICY #: 800.02	**CATEGORY:** Compliance and Ethics
System Approval Date: 3/15/18 **Site Implementation Date:** 4/25/18	**Effective Date:** **Last Reviewed/Approved:** 7/2015
Prepared by: Office of Corporate Compliance	**Notations:** N/A

GENERAL STATEMENT of PURPOSE

The purpose of this policy is to establish general requirements for authorizing access to, or the use or disclosure of, Protected Health Information ("PHI") for purposes of providing patients the ability to access and obtain a copy of their health information. The provisions contained in this policy and in all Northwell Health policies regarding PHI apply equally to the PHI of Northwell Health employees who also are, or have been, patients of Northwell Health.

POLICY

When an authorization is required, Northwell Health patient or the patient's personal representative must authorize access to, or the use or disclosure of, their PHI by fully executing and submitting the Health System's "Authorization for Release of Protected Health Information Pursuant to HIPAA" form ("Authorization Form"). This policy is subject to limited exceptions, as outlined herein.

SCOPE

This policy applies to all Northwell Health employees, as well as medical staff, volunteers, students, trainees, physician office staff, contractors, trustees and other persons performing work for or at Northwell Health; faculty and students of the Donald and Barbara Zucker School of Medicine at Hofstra/Northwell conducting research on behalf of the Zucker School of Medicine on or at any Northwell Health facility; and the faculty and students of the Hofstra Northwell School of Graduate Nursing and Physician Assistant Studies.

DEFINITIONS

Protected Health Information ("PHI"): Any oral, written, or electronic individually identifiable health information. PHI is information created or received by Northwell that (i) may relate to the

past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the payment for the provision of health care to an individual; and (ii) identifies the individual who is the subject or based on which there is a reasonable basis to believe that the individual who is the subject can be identified. The Health Insurance Portability and Accountability Act (HIPAA) further clarifies that PHI includes information that identifies the individual by one or more (depending on context) of the following 18 identifiers:

1. Names;
2. Geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code in certain situations;
3. All elements of date (except year) for dates directly related to an individual, including birth date, discharge date, date of death; and all ages over 89 and all elements of dates indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
4. Telephone numbers;
5. Fax numbers;
6. Electronic mail addresses;
7. Social security numbers;
8. Medical record numbers;
9. Health plan beneficiary numbers;
10. Account numbers;
11. Certificate/license numbers;
12. Vehicle identifiers and serial numbers;
13. Medical Device Identifiers;
14. Web Universal Resource Locators (URLs);
15. Internet Protocol (IP) address numbers;
16. Biometric identifiers, including finger and voice prints;
17. Full face photographic images and any comparable images; and
18. Any other unique identifying number, characteristic, or code.

Personal Representative: means the individual who, for decision-making purposes, will be treated as the patient. Depending upon the facts and circumstances of each case, a "personal representative" may be directly appointed by the patient or may be deemed to serve the role of "personal representative" under applicable laws and regulations.

PROCEDURE/GUIDELINES

General Right

The Privacy Rule requires covered entities such as Northwell Health to provide the patient or the patient's Personal Representative, upon request, with access to their protected health information. This includes the right to inspect or obtain a copy, or both, of the PHI maintained by the covered entity, as well as to direct the covered entity to transmit a copy to the designated person or entity of the individual's choice. Patients have the right to access PHI maintained by the covered entity, or by a Business Associate acting on behalf of the covered entity. The

covered entity must also provide the patient or the patent's Personal Representative with access to the PHI in the form and format requested, if readily producible in that form and format, or if not, in a readable hard copy form or other form and format agreed to by the covered entity and the patient or patient's Personal Representative.

Requesting a Copy of the Medical Record

If the medical record is maintained on-site, a copy of the requested medical record, or portions of the medical record, will be made available to the patient or the patient's Personal Representative within 10 days of receipt of the validly executed Authorization Form. If the medical record is maintained off-site, the copy must be provided within 30 days. If the Health System is unable to comply within the 30 days, a one-time extension of an additional 30 days is allowed if the Health System notifies the patient or the patient's Personal Representative, in writing, of the date by which it will comply with the request. The one-time extension letter will be on file in HIM with the associated request.

Requesting an Electronic Copy of the Medical Record

If the medical record is maintained electronically by Northwell Health, the patient or the patient's Personal Representative may request an electronic copy of the medical record by submitting a validly executed Health System Authorization Form to the applicable Health Information Management department ("HIM"). (See Vital Document VD001 – Authorization for Release of Information Pursuant to HIPAA).

Northwell Health must provide the medical record, in the electronic format reasonably requested by the patient or the patient's Personal Representative, if Northwell Health maintains the record electronically. Where applicable and technologically and operationally feasible, the requested PHI will be saved on to an encrypted device, such as a flash drive, and password protected. If there are electronic links to data within the medical record, such data must also be provided to the patient or the patient's Personal Representative.

If a patient or the patient's Personal Representative requests an electronic copy of the PHI that Northwell Health maintains only on paper, Northwell Health will provide the patient with an electronic copy if it is readily producible electronically and in the electronic format requested.

If the electronic medical record is not readily producible in the electronic format requested by the patient or the patient's Personal Representative, Northwell Health must provide the medical record in a readable electronic format agreed to by Northwell Health and the patient or the patient's Personal Representative (e.g., Microsoft Word or Excel, text, HTML or text-based PDF). The Health System may choose to provide a summary rather than the complete record, if acceptable to the patient or the patient's personal representative.

Northwell Health must transmit the medical record (whether paper or electronic) to a person or entity designated by the patient or the patient's Personal Representative pursuant to a patient or the patient's Personal Representative's request, if the request is in writing, signed by the patient

or the patient's Personal Representative and clearly identifies the designated recipient (an electronic signature is acceptable).

Special Categories of PHI with Heightened Protection

The following categories of PHI are treated with heightened privacy protections:

- HIV/AIDS PHI (See Northwell Health Policy #800.52);
- Mental health-related PHI (See Northwell Health Policy #800.53);
- Substance abuse (Drug and Alcohol) PHI (See Northwell Health Policy #800.55);
- Minors (See Northwell Health Policy #800.54);
- PHI of deceased patients in certain circumstances (See Northwell Health Policy #800.51); and
- PHI accessed, used, or disclosed for research purposes (See Northwell Health Policy #GR094).

Requesting a Copy of Laboratory Test Results

Patients may request laboratory results over the phone, via fax and in person. The Authorization for Release of Health Information Pursuant to HIPAA form must be filled out by the patient or representative before laboratory results may be released. Laboratory results will not be provided over the phone but may be mailed or faxed. Alternatively, results may be picked up from the performing laboratory or from any Patient Service Center. Laboratory results are also available via the patient portal at https://northwell.followmyhealth.com. If any questions arise regarding the laboratory result request, questions may be escalated to the Medical Director of the Laboratory. These guidelines apply to all Northwell Health System Laboratories.

Copying Costs

The patient or the patient's Personal Representative will be charged the reasonable cost of photocopying, not to exceed the standard as defined by New York State and Federal regulations, and mailing the medical record and/or providing the medical record in an electronic format. However, a patient or the patient's personal representative will not be denied access to their medical record based on inability to pay. Requestors who seek records for the purpose of supporting an application, claim, or appeal for any government benefit or program are prohibited from being charged to obtain copies in both paper and electronic format.

Special Provisions for Mailing PHI

The Privacy Rule requires that covered entities apply reasonable safeguards when making these communications to protect PHI from inappropriate use or disclosure to unauthorized persons. These safeguards will vary depending on the mode of communication used. The following items provide guidance on reasonable safeguards to protect patient information from being impermissibly disclosed. Safeguards include, but are not limited to:

- Carefully checking name and address of intended recipient. Many names are similar; make sure you have the correct name for the intended recipient on the envelope.

Make sure the address on the envelope matches the correct address of the intended recipient.

- Carefully checking the contents of the envelope before sealing. Making sure the contents may be permissibly disclosed to the intended recipient or properly relate to the individual. Checking all pages to make sure records or material related to other individuals are not mistakenly included in the envelope.
- Checking the information showing on the outside of the envelope or through the address window. Make sure identifying information that is not necessary to ensure proper delivery is not disclosed.
- When doing mass mailings, doing a test run to ensure the system is properly performing and check, at least a sample of the mailings, for the accuracy of name and address of the intended recipients and the correct contents, as indicated above, before sending.

Special Provisions Related to Faxing PHI or other Electronic Transmissions of PHI

Prior to faxing, e-faxing or otherwise electronically transmitting PHI, all persons must ensure that reasonable and appropriate safeguards are in place to protect patients' privacy. When the communications are in writing, the patient information may be sent by mail, fax, or other means of reliable delivery. Safeguards include, but are not limited to:

- Carefully checking the fax number to make sure you have the correct number for the intended recipient. When manually entering the number, check to see that it has been entered correctly before sending.
- Confirming fax number with the intended recipient when faxing to this party for the first time or if the fax number is not regularly used.
- Programming regularly used numbers into fax machines. Check to make sure you are selecting the preprogrammed number for the correct party before sending.
- Updating fax numbers promptly upon receipt of notification of correction or change. Have procedures for deleting outdated or unused numbers which are preprogrammed into the fax machine.
- Carefully checking the contents before faxing or otherwise transmitting PHI electronically. Making sure the contents may be permissibly disclosed to the intended recipient or properly relate to the individual. Checking all pages to make sure records or material related to other individuals are not mistakenly included in the envelope.

Special Provisions Related to Texting or Electronic Mailing (E-mailing) of PHI

No PHI shall be transmitted via text messaging. Prior to e-mailing PHI, all persons must ensure that they are sending such e-mail while using encryption technology, in accordance with Health System Policy #900.11. There are two methods in which an encrypted e-mail may be sent when using the Health System e-mail system:

- By using the "Encrypt & Send" button, instead of the usual "Send" button; or

- By including the words "*PHI*" or "*SECURE*" in the subject line of the e-mail. For SIUH employees the word "XSecure" must be in the subject line of the e-mail. This will ensure encryption if the email is subsequently forwarded out of the network.

Prior to emailing PHI to a patient, all persons must ensure that the patient signs a Northwell Health email consent form thus acknowledging the risks of sending PHI via email. Such emails must be encrypted unless the patient specifically requests otherwise by specifically notating at the applicable location on the consent form (See *Consent to E-mail and Text Communications (VD032) and Electronic Communication Consent (Page 3 of the Authorization for Release of Protected Health Information Pursuant to HIPAA - VD001*).

All individuals shall also ensure that other reasonable and appropriate safeguards are in place to protect patients' privacy when e-mailing PHI. These safeguards are contained in other Health System policies, and include, but are not limited to:

- Not forwarding business-related e-mails to personal e-mail accounts;
- Not including PHI content in e-mail subject lines;
- Confirming e-mail addresses and/or members of distribution lists before sending any e-mail, especially those containing any PHI; and
- Including in any e-mail only the minimum necessary amount of PHI required to accomplish the intended purpose.

Special Provisions Related to Telephone Messages that Include PHI

Health System personnel may leave the minimum necessary information on a voicemail system, answering machine, or with a person who answers the phone at a number provided by the patient or the patient's Personal Representative.

In most cases, it will not be appropriate to leave medical information. Health System personnel should verify with the patient or the patient's Personal Representative how he or she prefers to receive information, or if it is acceptable to leave messages. If this is not possible, Health System personnel should use discretion, and should not disclose medical information.

Special Provisions Related to Delivering PHI by Hand

All individuals shall also ensure that other reasonable and appropriate safeguards are in place to protect patients' privacy when delivering PHI by hand. These safeguards include, but are not limited to:

- Carefully checking the contents before delivering the PHI. Making sure the contents may be permissibly disclosed to the intended recipient or properly relate to the individual. Checking all pages to make sure records or material related to other individuals are not mistakenly included.

Revocation of Authorization

A patient or the patient's personal representative may revoke an authorization to release PHI by submitting to his or her health provider or treating facility, at any time, a written instruction to

this effect. This revocation will be granted except to the extent that the Health System has taken action in reliance upon the patient or the patient's Personal Representative's validly executed Authorization Form, and except if the patient or the patient's Personal Representative's authorization was obtained as a condition of obtaining payment.

Review of Authorization by Health Care Provider: Denial Requirements

Upon receipt of a validly executed Authorization Form, a health care provider will evaluate whether there is any information within the patient's medical record that should not be released to the patient or the patient's Personal Representative based upon a risk of harm to the patient. Such information may include:

- Psychotherapy notes that are not maintained in the patient's medical record;
- If the designated record set is part of a research study that includes treatment that is still in progress, provided that the patient agreed to the temporary suspension of access when consenting to participate in the research.
- Information disclosed in confidence to a health care provider by someone other than the patient that has not been disclosed to any other person; and/or
- Information that, if disclosed, would pose physical or psychological harm to the patient or others.

If a patient or the patient's Personal Representative is denied access to any information, the patient or the patient's Personal Representative will be informed in writing of the denial and their right to appeal such decision. If the appeal concerns matters governed by New York State law, the Medical Record Access Review Committee ("MRARC") will conduct the appeal. The patient's record and a brief explanation of the denial will be provided to the MRARC within 10 days of their request. If the appeal concerns matters governed by HIPAA, a health care provider, who is not directly involved in the patient's care and was not involved in the denial, will conduct the appeal.

If Northwell Health does not maintain the PHI that is the subject of the individual's request for access, and Northwell Health knows where the requested information is maintained, Northwell Health must inform the individual where to direct the request for access.

Verification

Prior to any access, use or disclosure of PHI, Northwell Health must exercise professional judgment to verify the identity of the individual requesting the PHI and the authority of any such individual to have access to the PHI, which may include obtaining documentation, statements or representations, whether oral or written. Northwell Health should only access, use or disclose PHI if acting on a good faith belief that the requesting individual's identity and authority has been verified.

Training

The Office of Corporate Compliance will provide HIPAA training on, at least, an annual basis

and as needed for any updates.

Sanctions

In compliance with HIPAA, violations of this policy will be subject to disciplinary action as outlined in the Human Resources Policy and Procedure Manual and in the Bylaws, Rules and Regulations of the Medical Staff.

Documentation

The Health System facility must document the medical record(s) that are subject to restriction.

Any documentation generated in compliance with this policy will be retained for a minimum of 6 years from the date of its creation.

Applicability of Policy to PHI of Health System Employees who are also Health System Patients

The provisions contained in this policy, and in all Health System policies regarding PHI, apply equally to the PHI of Health System employees who also are, or have been, patients of the Health System.

Questions related to the approval or denial of requests for confidential communications or restrictions on access to, or the use or disclosure of, PHI should be directed to the facility Privacy Officer.

REFERENCES to REGULATIONS and/or OTHER RELATED POLICIES

- Final HIPAA Omnibus Rule (78 Fed. Reg. 5566)
- Health Insurance Portability and Accountability Act, 45 CFR Parts 160 and 164
- Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5 (Feb. 17, 2009)
- NYS Mental Hygiene Law §33
- NYS Public Health Law §18
- Northwell Health Human Resources Policy and Procedure Manual, Part 5
- Northwell Health Bylaws, Rules and Regulations of the Medical Staff
- Northwell Health Policy #100.25 – Health Care Proxy, Health Care Agent, Patient Representative and Support Person, and Caregiver Designation Policy
- Northwell Health Policy #800.42 – Confidentiality of Protected Health Information
- Northwell Health Policy #900.00 – Acceptable Computer Use Policy
- Northwell Health Policy #900.03 – Mobile Support Services Policy
- Northwell Health Policy #900.11 – Electronic Mail Acceptable Use
- Northwell Health Policy #900.11A – Email Communication with Patient's Consent
- Northwell Health System Policy #900.01 – Internet Usage Policy

- Northwell Health Policy #100.97 Record Retention and Destruction
- Northwell Health Policy #800.47 Disposal Policy for Protected Health and Confidential Health System Information
- Northwell Health System Policy GR094, Access, Use and Disclosure of Protected Health Information for Research
- Northwell Health - Human Resources Policy Part 5-3 Conduct in the Workplace/Progressive Discipline
- Federal Register Vol. 79 No. 25 Part II

CLINICAL REFERENCES/PROFESSIONAL SOCIETY GUIDELINES

ATTACHMENTS

FORMS

VD001 – Authorization for Release of Information Pursuant to HIPAA

APPROVAL:	
Northwell Health Policy Committee	02-22-18
System PICG/Clinical Operations Committee	3/15/18

Standardized Versioning History:
*= Northwell Health Policy Committee Approval; ** =PICG/Clinical Operations Committee Approval
*7/13/10 **9/23/10
*5/31/12 **6/21/12
*7/25/13 **8/15/13
*6/25/15 **7/16/15