

# Corporate Compliance Training



# Compliance Training

---

Welcome to Northwell Health's Compliance training program. Every year state and federal governments increase their enforcement of health care fraud and abuse laws by means of audits, investigations and information obtained from whistleblowers. The number of government audits has skyrocketed and will continue to grow. The fines and penalties for violations have increased dramatically. In fact, in 2015, the United States Department of Justice collected over \$3.5 billion in from False Claims Act fines and civil judgments alone.

**COMPLIANCE**

# Corporate Compliance Contacts

---

BY TELEPHONE:



- 24/7 Compliance HelpLine: (800) 894-3226
- Corporate Compliance Office Line: (516) 465-8097
- Corporate Compliance Fax Line: (516) 465-8996

BY EMAIL:



- Corporate Compliance Email:  
[CorporateCompliance@Northwell.edu](mailto:CorporateCompliance@Northwell.edu)



THE INTERNET/INTRANET:

- Reporting A Potential Issue: [www.northwell.ethicspoint.com](http://www.northwell.ethicspoint.com)
- Reviewing Policies: <https://intranet.northshorelij.com/NSLIJ/policies/Pages/default.aspx>

# Ethisphere – One of the world’s most Ethical Companies 5 years in a row

## Fostering a Culture of:

- Ethics
- Compliance and
- Transparency



## Doing the RIGHT THING

- Notifying Corporate Compliance right away



# The Code of Ethical Conduct

---

Northwell Health's Code of Ethical Conduct (The Code) emphasizes our commitment to compliance, which is demonstrated by our robust Compliance Program. The Code has five major elements:



- Our commitment to complying with the state and federal laws that govern health care, and to the Code of Ethical Conduct and Northwell Health policies and procedures. Certain Compliance policies and procedures will be highlighted during this program.
- Our commitment to our patients, to give them the highest quality care possible at all times, to respect their choices, to safeguard patient information and to provide proper emergency care.
- Our commitment to the government regulators to comply with all coding and billing rules, to accurately document care in medical records, to cooperate with audits and investigations and to deal honestly at all times with accrediting bodies.

# The Code of Ethical Conduct (cont'd)

---

- Our commitment to our business partners to treat them fairly, to ensure that they operate both in an ethical manner and in compliance with our policies and procedures, and,
- Our commitment to our colleagues and to Northwell Health to avoid conflicts of interest; maintain a fair and respectful work environment and to make certain that we do not employ individuals who have been excluded from participation in the federal and state health care programs.

The Code can be found on “My Intranet” on the Office of Corporate Compliance webpage and should be reviewed in its entirety. In the event that you are not able to access “My Intranet,” please call the Office of Corporate Compliance at: (516) 465-8097.



# Northwell Health's Commitment to Ethical Conduct

---

Hopefully, you have heard that Northwell Health has been named one of the world's most ethical companies for the third consecutive year by the Ethisphere Institute. The Institute honors those organizations that have had a major impact on the way business is conducted by fostering a culture of ethics, compliance and transparency at every level of the company.

So let's keep up the good work by continuing to make ethics a top priority.



# Northwell Health's Policy on Gifts & Interactions With Industry

---

Northwell Health's policy on Gifts and Interactions with Industry which includes health care vendors such as pharmaceutical and medical manufacturers:



- Prohibits all gifts from Industry, regardless of value, including food
- Prohibits Industry-sponsored speakers' bureaus unless certain conditions are met
- Requires Industry representatives to visit our facilities by invitation only (permission must be granted by Northwell Health's Office of Procurement or the Chief Pharmacy and Medical Safety Officer)
- Requires that all consulting and other engagements with Industry be conducted according to the standards set forth in the policy
- Prohibits Industry-sponsored meals in connection with education programs, unless an exception applies
- Requires Industry support for research to comply with policies of the Feinstein Institute and the Office of Grants and Contracts
- Prohibits direct payments to individuals for Northwell Health projects
- Prohibits co-marketing arrangements with Industry
- Prohibits workforce members from soliciting gifts or other benefits from Industry

# Northwell Health's Policy on Gifts & Interactions With Industry (cont'd)

---

## Voluntary Physicians:

Northwell Health Policy on Gifts & Interactions with Industry (Policy #800.04) applies to interactions between Industry and employed and contracted physicians both on campus and off-campus.



**Voluntary physicians are covered on- and off-campus if they have faculty appointments or a connection to Northwell Health such as committee memberships or contract relationships.** Voluntary physicians are not covered off-campus if their contact with Northwell Health is limited to that of membership on the medical staff of a Northwell Health facility.

Please consult Northwell Health Policy #800.04, “Gifts and Interactions with Industry” for additional information. You can call **the Office of Corporate Compliance at (516) 465-8097** if you have questions. Please note that other arrangements with Industry may be permissible but **must be approved before services are provided.**

# Conflicts of Interest

---

- Northwell Health also has policies relating to conflicts of interest and gifts and interaction with industry. We have a strict ban on gifts of any type or value from health care industry vendors. Certain individuals are required to complete an external interest disclosure form annually and to update that form whenever they enter into a new financial or other relationship that might create a conflict with their position at Northwell Health.
- It is important to remember that even if you are not required to fill out the annual external interest disclosure form, you must disclose to the Office of Corporate Compliance any situation that may create a conflict of interest.
- Our policy also does not allow pharmaceutical sales reps to access our facilities unless they make an appointment with our Office of Procurement or our Chief Pharmacy and Medical Safety Officer.
- Please see Northwell Health's **policy #800.04, Gifts and Interactions with Industry**, for the most current information regarding Gifts and other interactions with Industry vendors. In addition to the Gifts and Interactions with Industry Policy, please also consult Policy #800.03, "Conflict of Interest and Recusal" and #GR065, "Review and Management of Conflict of Interest."

## Disclose A Potential Conflict If You or Family Members Are:

- ✓ Owner, part-owner, employee or otherwise receive compensation
- ✓ From a company that does business with Northwell Health
- ✓ From a company that seeks to do business with Northwell Health
- ✓ From a company that solicits employees of Northwell Health

# Conflicts of Interest in Research

- Individuals responsible for the design, conduct or reporting of research
- Serve on institutional research review committees
- Disclose external interests within 30 days of acquiring a new significant interest in order to comply with federal and state laws.
- Policy *GR065 Review and Management of External Interests in Research*
- A review by the office or COI Committee as necessary may take place prior to the proposed research activity
- Policy 800.70 Review and Management of Institutional Financial COI

# The Physician Sunshine Act

---

The Open Payments or Physician Sunshine Act, requires health care industry vendors, such as pharmaceutical and medical device companies, to report anything of value over \$10 provided to a physician or teaching hospital. The federal government is making all of this information public on its website in the interest of transparency. It is even more important that our workforce members follow our policy to ensure only appropriate payments get reported to the federal government.

All Northwell Health physicians are strongly encouraged to check the CMS website even if you do not believe you received any industry payments. Since the program is new, we anticipate some data errors. It is important that you confirm the accuracy of any data linked with your name as it can impact your reputation.

You can review your industry payments by entering your demographic information on the [Open Pay](#) section of the CMS website. If you have technical issues registering on the CMS website or disputing a payment, call the CMS help line at 1-855-326-8366.



# Important Compliance-Related Federal & State Laws - The Deficit Reduction Act and the False Claims Acts

---

The Deficit Reduction Act of 2005 requires Northwell Health to train our applicable workforce on the federal and state False Claims Acts and other laws that protect whistleblowers against retaliation.

The federal and state False Claims Acts establish liability when any person or entity receives payments from the government. **If the person or entity knowingly submits false claims to the government, then they are liable for penalties and damages for each false claim.** NY State also has a false claims act that is very similar to the federal law.

Anyone who has direct and independent knowledge of false claim activity can file a lawsuit on behalf of the government to recover money paid for the false claim. The person who files the suit is known as a whistleblower. If the lawsuit is successful, the whistleblower receives a share of the money recovered. It is illegal to retaliate against anyone who files a False Claims Act lawsuit by, for example, firing the whistleblower. Northwell Health has a strong no retaliation policy.

# Whistleblower

---

- A whistleblower is a person who exposes information or activity that is deemed illegal, dishonest or violates professional or clinical standards.
  - Persons who report false claims or bring legal actions to recover money paid on false claims are protected from retaliation.
  - You can learn more about these laws and about how whistleblowers are protected against retaliation by reading Northwell Health Policy #800.09, “Detecting and Preventing Fraud, Waste and Abuse.”
- 
- **Policy 800.09, Detecting and Preventing Fraud, Waste and Abuse**

# The False Claims Act

---

Under the new federal health care legislation, the federal False Claims Act has been amended to add a new basis for liability. If a health care provider fails to return an overpayment within 60 days of identification, this can constitute a false claim.

This means that any time Northwell Health knows that it has received an overpayment, the money must be returned to the government no later than 60 days after the overpayment was identified. If not, Northwell Health could be subject to false claims liability - which includes the amount of the overpayment, which can be tripled by the court, additional monetary penalties and other sanctions.

Please refer to Northwell Policy **#800.07**, “Compliance with Government Funded Health Care Claims and Cost Reporting Requirements” and Policy **#800.09**, “Detecting and Preventing Fraud, Waste and Abuse. This policy and all other policies referred to in this presentation can be found on “My Intranet” on the Office of Corporate Compliance webpage. In the event that you are not able to access “My Intranet,” please call the Office of Corporate Compliance at (516) 465-8097.

# The False Claims Act (FCA)

---

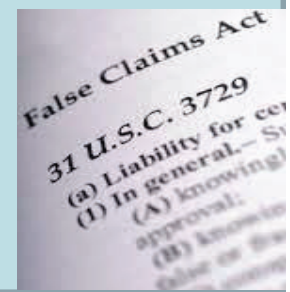
- The civil provisions of the FCA make a person liable to pay damages to the Government if he or she knowingly:
  - Conspires to violate the FCA;
- Carries out other acts to obtain property from the Government by misrepresentation;
- Knowingly conceals or knowingly and improperly avoids or decreases an obligation to pay the Government;
- Makes or uses a false record or statement supporting a false claim; or  
Presents a false claim for payment or approval.  
  
For example, a Medicare Part C Plan in Florida;
- Hired an outside company to review medical records to find additional diagnosis codes that could be submitted to increase risk capitation payments from the Centers for Medicare & Medicaid Services;
- They were informed by the outside company that certain diagnosis codes previously submitted to Medicare were undocumented or unsupported;
- Failed to report the unsupported diagnosis codes to Medicare; and  
  
Agreed to pay \$22.6 million to settle FCA allegations

# The False Claims Act (cont'd)

---

## Examples of false claims include:

- ✓ Billing for a higher level of services than were actually performed
- ✓ Billing for services that were not medically necessary
- ✓ Submitting a claim under one patient's name when services were provided to another person
- ✓ Altering claims forms or medical records
- ✓ Billing for services provided by an unlicensed provider
- ✓ Submitting false or inaccurate pricing or rebate information on pharmaceuticals to a federal health care program
- ✓ Enrolling a beneficiary in a Medicare Advantage program without the beneficiary's consent



# Fraud, Waste and Abuse

---

Financial and reputational damage can be extreme



In 2018, both federal and State governmental agencies continue to take an aggressive stance in protecting taxpayer-funded healthcare programs from fraud, waste and abuse. In Fiscal Year 2017, the Department of Justice collected more than \$3.7 billion dollars False Claims Act cases and more than \$56 billion since 1986. **It is important to know that government officials are increasingly likely to take executives and other individuals involved in corporate fraud, waste and abuse to court.**

In 2016 Tenet Healthcare paid over five hundred thirteen million dollars to settle fraud charges involving paying kickbacks to refer pregnant undocumented Latina women to Tenet facilities for care.

Earlier this year, the owner of a Nassau County Pharmacy was arrested and charged with Medicaid fraud. The Attorney General's Medicaid Fraud Control Unit filed an asset forfeiture request and are seeking \$8.7 million dollars in damages and penalties. They have alleged that the owners of the Pharmacy paid kickbacks to a hospital employee for prescription referrals for cancer medications as well as billing Medicaid for a million dollars' worth of

# Fraud, Waste and Abuse

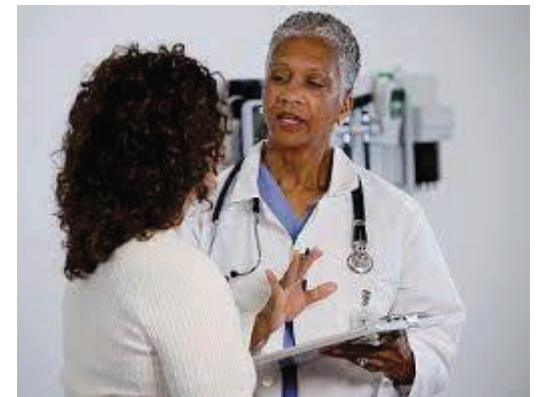
---

- **Fraud** is knowingly and willfully executing, or attempting to execute, a scheme or to intentionally deceive or defraud any health care benefit program, government contractor or payor.
- **Waste** includes overusing services, or other practices that, directly or indirectly, result in unnecessary costs to the Medicare Program. Waste is generally not considered to be caused by criminally negligent actions but rather by the misuse of resources.
- **Abuse** includes actions that may, directly or indirectly, result in unnecessary costs to the Medicare Program. Abuse involves payment for items or services when there is not legal entitlement to that payment and the provider has not knowingly and/or intentionally misrepresented facts to obtain payment.

# Fraud, Waste and Abuse

---

- There are differences among fraud, waste, and abuse. One of the primary differences is intent and knowledge. Fraud requires intent to obtain payment and the knowledge that the actions are wrong. Waste and abuse may involve obtaining an improper payment or creating an unnecessary cost to the Medicare Program, but does not require the same intent and knowledge.
- There are additional laws that address fraud, waste and abuse that we must comply with.





# The Anti-Kickback Statute

---

The Anti-Kickback statute prohibits payments by Northwell Health to any referral source for the purpose of receiving referrals of patients, or services that are reimbursed by Medicaid, Medicare or any other federal or state health care program. **Here at Northwell Health we do not pay for referrals and we do not accept payment of any kind for making or receiving patient referrals from other health care providers. Instead, we accept patient referrals and admissions based solely on the patient's medical needs and on our ability to render medically-necessary services.**

Under the law, prohibited kickbacks include not just giving money to physicians or other referral sources, but also any kind of gift or benefit or anything of value. If you have any questions about the Anti-Kickback statute, please consult the Office of Corporate Compliance at (516) 465-8097.



# The Stark Law

---

Another important federal law is the Stark Law. **This law specifically prohibits physicians from referring patients to certain healthcare entities in which the physician or the physician's family member has a financial interest.** There are certain exceptions contained in the law. If a financial relationship with a physician is not properly structured and administered, legal violations for Northwell Health and the individual may result.

**In particular, please note that Northwell Health cannot provide more than \$392 per year in non-monetary compensation or cash equivalents to non-employed physicians unless certain exceptions apply.** Non-monetary compensation includes such items as meals at restaurants, gift cards, golf outings and condolence or congratulatory gifts.

Please consult and follow Northwell Health Policy #800.10, "Business Courtesies to Potential Referral Sources," #800.12, "Potential Referral Sources," and #800.14, "Office Space and Equipment Leases with Physicians and Others."



# Exclusion Screening For Providers

---

Federal law requires that Northwell Health screen all of our employees, trustees, physicians, volunteers and vendors on a regular basis to ensure that Northwell Health does not do have any excluded providers on our staff. **Excluded providers cannot bill federal or state health care programs, either directly or indirectly.**

Here at Northwell Health, we screen our employees, vendors, trustees, voluntary physicians and volunteers on a monthly basis. If you are excluded from participation in any federal or state health care program, you must immediately inform the Office of Corporate Compliance. Failure to do so can result in severe sanctions.



# Value Based Purchasing Programs

---

- Delivery System Reform Incentive Payment Program (DSRIP)
- Accountable Care Organization (ACO)
- Bundled Payment for Care Improvement Program (BPCI)

**The right care at the right time**

# Accountable Care Organization

---

- Must maintain a Compliance Program
- Prevent and detect incident's related to fraud, waste and abuse
- A distinct Code of Ethical Conduct
- Direct questions to the ACO's Compliance Officer at 516-465-8097
- ACO 24 hour Help Line - 800-894-3226 - Anonymous reporting

# Accountable Care Organization Requirements

---

- Must notify patients of your participation in an ACO
- Conspicuous placement of approved signage
  - We recommend the lobby of the practice
- Signage must describe what an ACO is, how it may benefit the patient and opt-out information if the patient chooses
- Copy of the Beneficiary Information Notice may be provided to the patient
- Contact the ACO directly at 1-800-381-6140 to order signage and/or Beneficiary Information Notices

# Accountable Care Organization and Patient Interaction

---

- Medicare fee-for-service patients continue to maintain the freedom to receive services from providers of their choosing even if the provider is outside the ACO
- ACO providers may encourage and explain the benefits of coordinated care through the ACO to patients

**Example:** Receiving radiology exams from an ACO provider may allow the provider quicker access to the study results



# Accountable Care Organization and Patient Interaction

---

- In limited circumstances, providers may arrange for free or discounted items or services if it relates to the patient's care or encourages health awareness

**Example:** ACO or its providers may give a patient a blood pressure monitor as a means to encourage the patient to monitor their blood pressure

- The ACO may never give patients cash or other items unrelated to health care
- The ACO and its providers may not reward patients for either receiving care from the ACO or for staying in the ACO or as a means of persuasion to remain

**Example:** The ACO may not generally waive or reduce Medicare co-payments or deductibles



# Accountable Care Organization and Patient Interaction

---

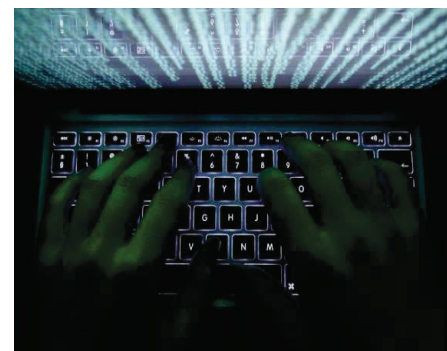
- The ACO cannot avoid patients who may drive up healthcare costs. CMS has indicated that they will monitor for patterns that would suggest that the ACO or its providers are steering at-risk beneficiaries away from the ACO



# Accountable Care Organization Data Use Agreement

---

- The ACO has signed a Data Use Agreement (DUA) allowing them to receive patient data directly from CMS to assist in meeting the goals of the Program
- Handling and use of the patient data under the DUA differs somewhat from how we handle protected health information under HIPAA
- Use of the data is limited to furthering the goals of the ACO and any request must be limited to the minimum amount necessary to achieve the intended goal
- The data may not be shared outside of the ACO without the approval of CMS



# Accountable Care Organization

---

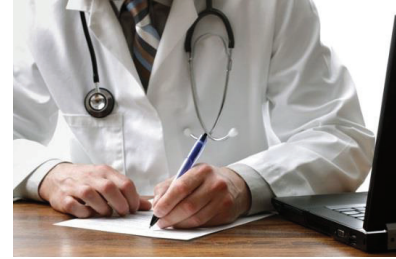
- The ACO may receive a portion of any shared savings based upon the accurate data that it is required to submit to CMS
- The ACO is required to retain all records related to the ACO for a 10 year period from the completion of its involvement in the Medicare Shared Savings Program
- This may differ from other record retention requirements that you may have and care should be taken not to destroy any data that may be relied upon by the ACO in its reporting efforts

# Accountable Care Organization and Bundled Payment for Care Improvement Program (BPCI)

---

- Both the ACO and BPCI provider is obligated to report probable violations of law as it relates to our involvement in the Program
- We are all responsible for ensuring that we are delivering excellent patient care that conforms to the rules and regulations set forth by various government regulators
- Examples of things that should be reported to the ACO or BPCI Compliance Officer include any allegations of fraud, waste or abuse related to or impacting the ACO operations, government investigations or inquiries concerning the ACO, patient privacy concerns, potential conflicts of interest, patient complaints alleging inappropriate behavior of ACO or BPCI providers, suspected violations of the ACO's Code of Ethical Conduct, and any other compliance concern

# Documentation



Documentation is one of the most critical functions a physician may perform. It is the foundation of the quality of care we provide to our patients and ensures accuracy of continuity of care as well

## Importance of Accurate Medical Records

- Every medical professional and medical practice needs to keep accurate documentation
- It is necessary for the protection of the medical practitioner as well and reduces malpractice exposure
- It is crucial to the quality and continuity of patient care

# Key Points in Documentation

- Legibility is important, but luckily with today's EMR, this becomes less of an issue
- Be sure to document all of the elements necessary for the visits and procedures you perform so you may bill appropriately for those services
- Medical necessity is key when billing for the level of service
- Level of specificity is very important for ICD-10-CM accuracy
- All notes in the medical record require a signature by the billing provider



# Policies and Procedures

There are many Policies you may access through the intranet for most coding, billing and documentation issues and/or questions. Some of the policies include:

- 800.20 - Physician Signature Requirements
- 800.21 - Physicians at Teaching Hospitals (PATH) Supervision and Billing Policy
- 800.49 - Inpatient and Outpatient Facility and Professional Coding Compliance Policy
- 800.50 - Billing Compliance Policy
- 800.63 - Copy and Paste Notes in the Electronic Medical Record
- ORSL.4002 - Kyphoplasty/Vertebroplasty, Indications and Limitations

If you have any questions, please contact the Office of Corporate Compliance for clarification

# The Health Insurance Portability & Accountability Act (HIPAA)

---



One of the hottest issues today in Compliance is the Health Insurance Portability and Accountability Act, which is known as HIPAA. The government is very serious about health care providers and their workforce members complying with HIPAA. Failure to follow the HIPAA rules can result in serious fines and individuals can even be sent to jail for merely looking at a medical record they were not authorized to view.

All health care providers are required to notify the federal government when confidential patient information is accessed, used or disclosed improperly unless the health care provider can demonstrate that there is a low probability the protected health information was compromised. This is a much stricter standard than in years past. The fines and penalties for violations of HIPAA are now enormous - up to \$1.5 million per violation. The media routinely publicizes instances where patient data is lost, stolen or otherwise improperly acquired.



# The Health Insurance Portability & Accountability Act (HIPAA) (cont'd)

---

## Real World Examples:

- Recently, a Florida Emergency Department staffer was sentenced to 12 months in federal prison for inappropriately accessing 760,000 electronic health records and then selling information about motor vehicle accident patients to an individual co-conspirator, who used the data to solicit business.
- Similarly, two employees of Jamaica Hospital Medical Center were recently charged with illegally accessing emergency room patients' medical records and personal identification information, and selling that data to individuals who then solicited services such as outpatient care or legal assistance - sometimes while patients were still in the ER. "These defendants are accused of blatantly violating their HIPAA obligations and illegally trolling through confidential patient records. Their alleged actions led to patients who were seeking treatment for injuries unwittingly being victimized again with the illegal release of their personal information and medical records," said DA Richard Brown. These media reports hurt healthcare providers' reputations.

Here at Northwell Health we have to redouble our efforts to ensure that all patient information is kept confidential and is used only for appropriate purposes by authorized individuals.

# Protecting Our Patients' Data

---

- It's our job to protect the privacy and secure the data of each and every one of our patients.



When a patient enters any of our facilities, the first thing they encounter is our registrar. This person is likely a total stranger to them or maybe they are acquainted, but the patient proceeds to provide our employee with the most intimate and sensitive information they will ever share with anyone. Our patients should never have to wonder what happens to their personal data once it's provided to us. They should be concentrating on their health and nothing more. It's our job to protect the privacy and secure the data of each and every one of our patients. If we fail at privacy, that's the story the patient walks away with.

You are expected to know what is required of you in order to protect our patients' privacy and secure our data.

Please pay close attention to the remainder of this training, so you have the knowledge you need. If you have any questions about patient privacy at any time, please contact Corporate Compliance. Our contact information will appear at the end of this training.

# The HIPAA Privacy Rule & Elements of PHI

---

The HIPAA Privacy Rule puts restrictions on the uses and disclosures of protected health information (PHI). PHI is all individually identifiable information about a patient's health care services or payment rendered for those services. PHI comes in many forms, including oral, written and electronic. Any communication of PHI is covered by HIPAA.

## There are 18 Elements of PHI:

1. Name
2. All Geographic Information Smaller than State
3. Elements of dates (except year)
4. Telephone Number
5. Fax #
6. Email Address
7. Social Security Number
8. Medical Record Number
9. Health Plan Beneficiary Number
10. Account Number
11. Certificate/License #
12. Device Identifiers / Serial Numbers
13. Web URLs
14. IP Addresses
15. Biometric Identifiers
16. Full Face Comparable Images
17. VIN, Serial Number, License
18. Any Other Unique Identifying Number, Characteristic or Code



# HIPAA is not intended to hinder patient care, but use reasonable precautions when sharing information

---

The HIPAA Privacy rule is not intended to prohibit providers from talking to each other or to their patients. Reasonable precautions must be used to avoid sharing patient information with those not involved in the patient's care. Use discretion when speaking about a patient. For instance, don't talk in hallways or visitor access locations, lower your voice when discussing patient information in person or over the phone, and avoid conversations about one patient in front of other patients or their visitors.



Additionally, we recognize the integral role that family and friends play in a patient's health care. The HIPAA Privacy Rule allows routine and often critical communications between health care providers and these persons. A practitioner may ask the patient's permission to share relevant information with family members or others and give them an opportunity to agree or object. A common example would be situations in which a family member or friend is invited by the patient and is present in the treatment room with the patient and the practitioner when a disclosure is made. For more information on what can be discussed with family and friends, visit the Corporate Compliance website.

# HIPAA - Use and Disclosure of PHI

---

PHI may be accessed, used or disclosed only when specifically permitted by HIPAA. All other uses or disclosures are prohibited. Please refer to Northwell Health Policy #800.02, “Use, Access and Disclosure of PHI with Valid Authorization” and Policy #800.42, “Confidentiality of Protected Health Information.”

- **Treatment:** It is important to note that PHI may always be used for treatment of a patient. No authorization or consent by the patient is required for this use. The **Minimum Necessary Rule** discussed above does not apply to the use of PHI for treatment. Generally, the Privacy Rule permits disclosure of PHI to an individual who is involved in the patient’s care, so long as the patient does not object to this disclosure.
  - The HIPAA Privacy rule is not intended to prohibit providers from talking to each other or to their patients. Reasonable precautions must be used to avoid sharing patient information with those not involved in the patient's care. Use discretion when speaking to a patient. **For instance, don’t talk in hallways or visitor access locations, lower your voice when discussing patient information in person or over the phone, and avoid conversations about one patient in front of other patients or their visitors.**



# HIPAA - Use and Disclosure of PHI (cont'd)





- **Payment:** In general, PHI also can be used to obtain payment for health care services rendered to the patient, for health care operations, when requested by the patient or when required by law. *The law does contain some exceptions to these general rules so be sure to contact the Office of Corporate Compliance if you have any questions.*
  
- **Friends & Family:** Additionally, we recognize the integral role that family and friends play in a patient's health care. The HIPAA Privacy Rule allows routine and often critical communications between health care providers and these persons.
  - *Living Patient:* A practitioner may ask the patient's permission to share relevant information with family members or others, may tell the patient he or she plans to discuss the information and give them an opportunity to agree or object, or may infer from the circumstances, using professional judgment, that the patient does not object. A common example of the latter would be situations in which a family member or friend is invited by the patient and present in the treatment room with the patient and the practitioner when a disclosure is made.
  - *Deceased Patient:* Since 2013, PHI may now be released to family members and others who were involved in the care, or payment for care, of a deceased patient prior to death, unless doing so is inconsistent with any prior expressed preference of the deceased patient that is known to Northwell Health.



# HIPAA - Use and Disclosure of PHI (cont'd)

---

- 
- **Response Time:** HIPAA also requires us to provide a medical record to a patient no later than 30 days and Northwell Health is required to allow them to inspect their medical record in a timely manner. HIPAA now requires health care providers to also try to provide a medical record in a patient's desired format. If Northwell Health maintains the medical record in an electronic format, Northwell Health is required to provide it to the patient in an electronic format if requested and is readily available in that format. If not we must provide a hard copy or other format agreed to by the patient. Please see Policy #800.02, "Release of Protected Health Information for Living Patients" for more information.

- 
- **Research:** PHI can be used for research. However, it can be used only with the approval of an authorized Institutional Review Board (IRB) and with either informed consent and authorization, a waiver of informed consent or authorization, or under a data use agreement as determined by the IRB. You can contact the Office of the IRB at (516) 562-3100 for more information or go to <http://www.feinsteininstitute.org/professionals/resources-for-investigators/administrative-services/human-research-protection-program/forms/> for an application.



# HIPAA - Use and Disclosure of PHI (cont'd)

---



➤ **Immunization Records:** Since changes to the HIPAA law in 2013, medical providers can now release the immunization records of patients enrolled in educational institutions that are required by New York State to have such information, as long as the provider obtains permission for the release of the records from the patient or from the patient's parent or guardian, if the patient is under 18 years of age. The law no longer requires the medical provider to obtain written permission before the information can be released.

➤ **Not all** of the regulations released in 2013 made it easier to disclose PHI. Many of the regulations actually made it more difficult for medical providers to use or disclose PHI without written authorization from the patient. For example, the new HIPAA regulations now place severe limitations on the ability of medical providers to sell PHI or to use PHI for marketing purposes.


- **Selling / Marketing PHI:** Northwell Health has a general prohibition against selling the PHI of patients, and it will only do so in very limited circumstances if it has a prior written authorization from the patient. Northwell Health must also obtain a patient's authorization using a HIPAA-compliant authorization form before using or disclosing the individual's PHI for Marketing purposes.





# HIPAA - Destruction of PHI

---

- An extremely important point to remember about PHI is that it MUST be thrown in shredding bins and NEVER in a trash receptacle. If you're not sure if a document contains PHI, always lean on the side of caution and shred!
- 
- Old equipment such as CDs, old workstations or laptops and USB drives need to be discarded properly when you are ready to dispose of them. Dispose of old media and equipment by calling the IS Service Desk at (516,718,631) 470-7272 for proper removal.
  - Hardcopy data in non-paper form (e.g., microfilm, microfiche, imaging films) cannot be discarded in confidential document bins designated for paper waste only and thus any PHI, PII or other sensitive or highly sensitive information on such non-paper form must be rendered unrecognizable and properly discarded either internally or through a Northwell Health approved and contracted vendor.
  - For more information on proper disposal of PHI, see Policy #800.47, "Disposal of Protected Health and Confidential Information."

# HIPAA Security Rule

---

The HIPAA Security Rule protects electronic PHI and sets standards for the electronic transmission of PHI. The Security Rule provides **three** types of safeguards:

- 1) The administrative safeguards set limits on who may access PHI electronically. It also requires detection systems to detect and prevent security breaches and ongoing evaluations and audits of computer systems' security.
- 2) The physical safeguards required by the Security Rule include facility access controls, such as ID badges, which must be worn at all times. The Security Rule also requires device and media controls to track hardware.
- 3) The technical safeguards include software to monitor for viruses, the encryption of data and system tracking of log on attempts.



# HIPAA Security Rule - Technical Safeguards (cont'd)

---

## Technical Safeguards:

- **Access Control** - everyone must have a unique ID and password; never share it
- **Emergency Access** - electronic records must be accessible at all times
- **Automatic Logoff** - after a certain period of inactivity, system should force a logoff
- **Audit Controls** - the ability to see who has accessed the patients' record
- **Integrity** - system checks to insure no data has been manipulated either unintentional or by an unwanted source
- **Person/entity authentication** - you are who you say you are (password, token or both)
- **Encryption protecting PHI at rest** - data is encrypted while stored where appropriate and reasonable
- **Encryption in transit** - data is encrypted while being transmitted

Northwell Health is working hard to ensure the security of our data through these safeguards and others.

---

## Use your Professional Judgment

Health care workers are reportedly suffering from "HIPAA phobia," a fear of giving too much information about a patient . The HIPAA privacy rule clearly states that "Health care providers may share information as necessary to identify, locate and notify family members, guardians, or anyone else responsible for the individual's care, of the individual's location, general condition or death. The health care provider should get verbal permission from individuals, when possible, but if the individual is incapacitated or not available, providers may share information for these purposes if, **in their professional judgment**, doing so is in the patient's best interest."

- Northwell Policy 100.75 - Communicating with Patients & Families about Serious Adverse Events
- Northwell Policy 800.58 - Facility Directory Opportunity to Agree or Object (Opt-Out)



# More Important Topics

---

Responding to government inquiries is simple. You should notify the Office of Legal Affairs immediately if any government agent appears on Northwell Health premises or calls and requests an interview with our employees and/or access to records. While you have a right to speak with the government directly if you so choose, we recommend that you contact Legal before doing so. You do not have a right to release Northwell Health documents to the government without authorization, so please contact Legal for guidance., if you have any questions. We have a policy to provide further guidance, Policy 800.48 Responding to Government Inquiries.

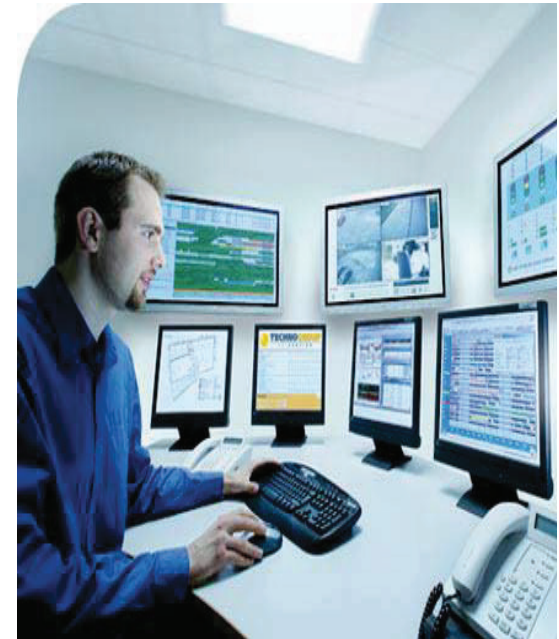
## Media Inquiries

- Also, please remember if the media ever requests to interview a patient, employee or vendor, please make sure you contact our Public Relations Department before agreeing to do anything including even acknowledging a patient is at our facility. They can be contacted at 516-321-6701.

---

## FairWarning is our patient privacy intelligence program that monitors our EMRs 24 hours a day

- Whether the patient is an employee, friend or family, everyone is entitled to their privacy when they are being cared for here. You only have the right to see a patient's data if your job requires you to do so. **Inappropriate access of medical records can result in disciplinary action.** Don't take the chance!
- As we've said, we are accountable for a lot of sensitive patient information. We are all aware, if information gets into the wrong hands, the patient could suffer medical and financial consequences. Don't forget, those patients include us, our families and our friends.
- Hopefully you now understand why it's so important to take ownership and protect our data.



# Monitoring our data for inappropriate use

---

FairWarning also helps prevent identity theft by alerting privacy staff of inappropriate access to medical records or Social Security numbers.

*“Identity Theft is not just a statistic; it is important to realize the numbers represent victims, the harm is serious, and it can impact victims’ ability to get a job, rent an apartment, or go to college.”*

*-Julie Ferguson, Identity Theft Resource Center Chair, Industry Expert*

Another way in which we protect our data is through the use of a Data Loss Prevention (DLP) application. DLP monitors for confidential data being downloaded, copied, emailed, printed or transmitted from Northwell devices.

# Protecting ePHI

---



Everyone at Northwell Health is responsible for protecting PHI. We are all responsible for protecting PHI, whether it's contained in a written document, stored on a portable device or a computer, or spoken about between workforce members in an appropriate context. Northwell Health's policies help us to do this by informing us about the safeguards and procedures that must be utilized to secure PHI.

Computer users must actively protect Northwell Health computers from loss or theft. It is very important that you keep track of your equipment and storage devices. Lock your computer whenever you are not using it.

All computers and mobile devices must be password-protected and use a screensaver wherever possible in accordance policy. You should store all of your documents containing PHI on network drives, not on your computer's hard drive.

**Never leave a computer or any device containing PHI - or paper PHI - in a car overnight. You should even remove the computer, device or files from the visible areas of your car during short stops. It only takes a minute for a thief to break into your car and take the PHI.**



# Use great care when emailing, faxing and mailing PHI

---

Also a lot of Northwell Health's protected health information either gets emailed, faxed or mailed to our patients and members as part of providing clinical care or for billing purposes.



It is our policy and a HIPAA requirement to get authorization from a patient before emailing them about their care. Our policy #800.02 Release of Protected Health Information for Living Patients, will guide you in handling patient emails and has an associated Email Consent form.

Also, verifying the correct name and address before emailing, faxing, scanning or mailing any patient or member communication is the best way to ensure you don't make an error. It is critical we get this right so a patient's information does not end up lost or with another person. Here is a checklist that the Office for Civil Rights recommends we follow to prevent any inadvertent errors when mailing and faxing.



# Northwell Policy #800.02 Release of Protected Health Information for Living Patients

---



- Carefully check name and address of the 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 check the contents of the envelope before sealing. Make sure the contents may be permissibly disclosed to the intended recipient or properly relate to the individual. Check all pages to make sure records or material related to other individuals are not mistakenly included in the envelope.
- Check 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.

# Faxing PHI



- Carefully check 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.
- Confirm fax number with the intended recipient when faxing to this party for the first time or if the fax number is not regularly used.
- Program regularly used numbers into fax machines. Check to make sure you are selecting the preprogrammed number for the correct party before sending.
- Update 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.
- Locate fax machines in areas where access can be monitored and controlled and avoid leaving patient information on fax machines after sending.
- Have policies and procedures in place to safeguard protected health information that is faxed, including processes to act promptly on (1) changes in fax numbers to ensure corrections are made in all the relevant records; and (2) reports of a misdirected fax to identify the cause and take steps to prevent future incidents, including revising the organization's policies and procedures.
- Train staff on the policies and procedures for the proper use of fax machines that your organization has put in place to safeguard protected health information during faxing. Update the training periodically and be sure to train new staff.

## Payment Card Industry Data Security Standards (PCI DSS)

- Northwell has developed credit card handling policies. These policies are located on our intranet site under the Information Services Privacy and Security policies: 100.009, 100.010 or 100.011
- There are many devices and tools marketed for credit card processing, however, some may not be compliant so please ask for help
- Avoid writing down credit card information wherever possible
- Always process credit card information received directly into the credit card terminal or credit card processing system
- If you must write it down then always shred any written credit card information after processing or always redact or black out the credit card number, or display only last the four digits if credit card information must be retained
- Do not store credit card information in any manner or in any system. For example, do not store the information in billing systems or in any other place or format.
- Never ask for or store credit card CSC/CVV or PIN code which is the three or four digits on back of card
- Never retain full credit card information after payments have been processed

## Payment Card Industry Data Security Standards (PCI DSS)

- Never send or receive credit card information via email, instant messaging, fax or any other medium
- Never pass around someone's credit card information or call other offices to process credit card transactions
- Never provide customer receipts showing more than the last four digits of the credit card number
- Periodically inspect credit card terminals to detect tampering or substitution of the device. Here are some examples of tampering devices that you can look for:



- Verify the identity of any third party persons claiming to be repair or maintenance personnel prior to granting them access to review, modify, replace or troubleshoot credit card processing devices
- Report suspicious behavior and indications of device tampering or substitution to the site manager, Internal Audit and Treasury
- IF YOU ARE NOT SURE OF WHAT TO DO PLEASE ASK!

**Cybercrime Scam**  
**Social Engineering**  
**Phishing**  
**Ransomware**  
**Cyberattack**  
**Insider Threat**



Cybercrime can occur when you...

- Open e-mail attachments or clicks on links from unknown senders
- Provide sensitive information (such as a username or password) without first verifying that the request is legitimate
- Fail to protect your passwords
- Send confidential information (such as PHI) in an unencrypted email
- Connect to an unsecured public wireless network to check Northwell email
- Post sensitive or confidential information to social media sites
- Neglect to follow security policies and procedures



- An insider is someone who would normally has access to systems and data but misuses their access
- The majority of data breaches in the healthcare industry are caused by insiders
- YOU can help protect Northwell against insider threats
- Follow our policies and stay vigilant
- If you see something, report it to your manager or the IS Service Desk at 516-470-7272



## **Social Engineering**

is the art of manipulating people so they give up confidential information

- Criminals may use social engineering schemes to gain access to your facility
- They may attempt to elicit passwords or other sensitive information
- Social engineering can occur on the phone, in person or via email
- Usually include a request for access or information



# Phishing



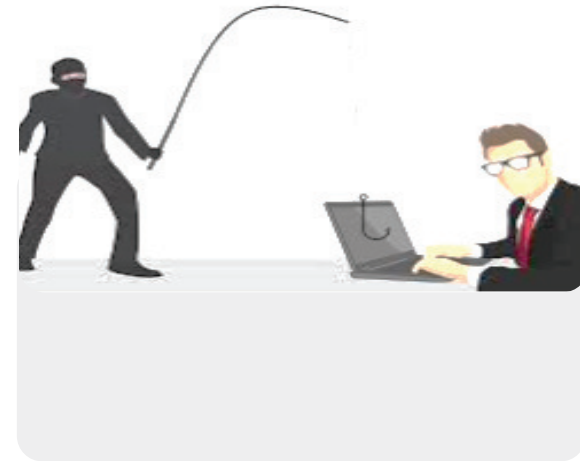
- One of the most common social engineering tactics used to access sensitive information and infect computer systems
- Phishing is a type of cyberattack where criminals send legitimate looking emails in an attempt to trick people into revealing private information such as usernames, passwords, or account numbers for fraudulent use
- Just clicking on a link, opening an attachment, or providing a username and password is all it takes to potentially compromise Northwell Health's systems and data
- But it's not just email...phishing can also occur via phone (also known as vishing –short for voice phishing) or through text (also known as smishing – short for SMS phishing)

## How Can I Stop Phishing Attempts?

Red flags include:

- Requests for sensitive information, such as your password or account number
- Unknown senders or unexpected links and attachments
- A sense of urgency, time limits or threatening language that tries to evoke strong emotion

If you receive a suspicious email that's asking you to click on a link or an attachment, demanding payment or urging you to provide confidential information- report it right away using the **Report Phishing** button in your Outlook application or by forwarding the email to [phish@northwell.edu](mailto:phish@northwell.edu)



# Cloud Security

Cloud sharing and storage services allow us to easily share and access files from home, work, and our mobile devices

- Only share the **minimum amount of information necessary and only with those who have a business need to know** the information
- Remove access when files are no longer needed
- When receiving shared files via OneDrive, especially those that are flagged as EXTERNAL, **always make sure that you recognize the sender and were expecting the file before you open the document**
- If you're not sure, **STOP** and contact the sender to verify whether they have, in fact, shared a file with you



## Protecting Information: Everyone is Responsible

- Use strong passwords and keep them safe
- Exercise caution when using social media
- When working remotely, make sure that you connect to the Northwell network securely (using vPortal), always maintain physical possession of your device, and never connect to unsecured public Wi-Fi networks
- Always keep your workstation secure by locking it using <CTL><ATL><DEL> before walking away
- If you're using a shared workstation, always remember to logoff before you leave
- Limit the amount of information you send and encrypt all emails that contain PHI or other sensitive information
- If you see something, make sure you say something. Report any incident, even suspected ones, without delay



# Drug Diversion

---

As you may be aware, prescription drug abuse has been a growing problem across our country and within Health Care itself. Drug diversion is described as abuse of controlled substances or the *illegal* use of a *legal* narcotic. Diversions pose a risk to patients, the abuser, Hospital or Health system and the public.

Some ways a drug can be diverted are;

- Directly from the hospital supply or Pyxis and Omnicell machines
- Directly from the patient by short dosing
- Substituting the entire dose
- Falsifying patient's medical record in either type of diversion
- Keeping "wasted" medicine and/or delivery equipment
- Retaining and using discarded medicine

# Drug Diversion



To report drug diversion issues, please call the Compliance Helpline at (800) 894-3226

24 hours a day, 7 days a week or go to:

[www.northwell.ethicspoint.com](http://www.northwell.ethicspoint.com)

Reports are confidential and can be anonymous

# The Emergency Medical Treatment & Active Labor Act

---



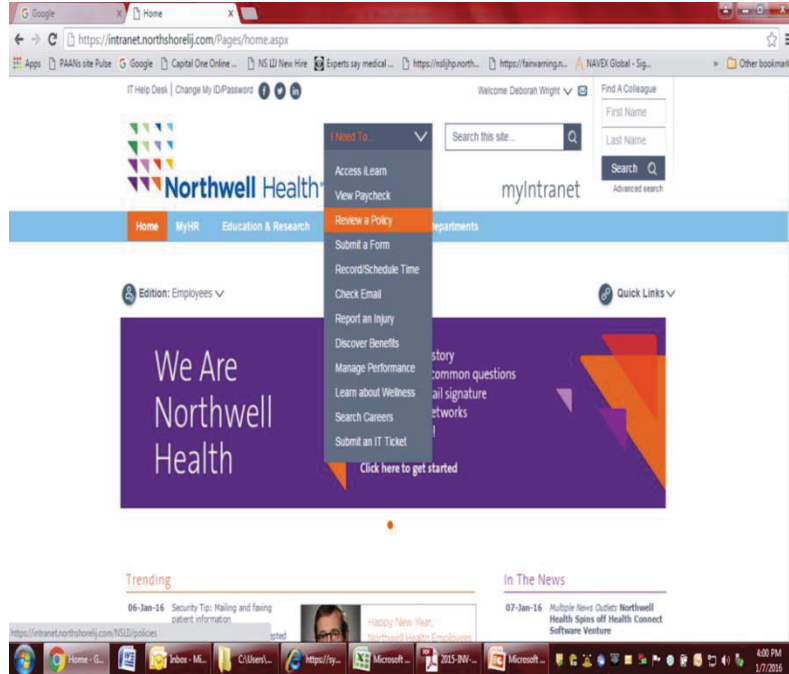
The Emergency Medical Treatment and Active Labor Act, known as EMTALA, applies to all individuals presenting to a dedicated emergency department. Anyone presenting to an emergency department requesting treatment for a medical condition is entitled to a medical screening examination.

This examination must be of sufficient scope to conclude, with reasonable clinical confidence, whether an emergency medical condition does or does not exist. The examination cannot be delayed while the patient's health insurance coverage and/or method of payment are verified. If the facility cannot treat the patient, the patient must be stabilized before being transferred to another facility. The receiving facility must have the capacity and the ability to provide the needed medical treatment.

The emergency department also must maintain certain records, including a central log, an on-call list of physicians and records of patient transfers for at least five years. Failure to follow these rules can result in fines and other penalties. Please refer to Northwell Health Policy #700.01, "Emergency Treatment, Stabilization, Transfer of Patients and EMTALA."

# How To Locate Important Policies

Northwell Health Policies can be easily located on the Northwell Health Intranet website by clicking on the “I Need To” and “Review a Policy” link at the following web address:  
<https://intranet.northshorelij.com/pages/home.aspx>



Please contact IS for additional support (516, 718,631) 470-7272

In the event you cannot access the Northwell Health Intranet website, you can also call the Office of Corporate Compliance at (516) 465-8097 to receive copies of all policies.



# Corporate Compliance HelpLine

---



The Compliance HelpLine is a service provided by an outside vendor to Northwell Health workforce members and patients. You can make a report by calling the HelpLine at **800-894-3226** or by going on-line to [www.northwell.ethicspoint.com](http://www.northwell.ethicspoint.com).

This service is available 24 hours a day, seven days a week. You can make an anonymous report or you can use your name or other contact information. All reports received on the HelpLine are investigated and resolved as appropriate. You cannot be retaliated against for using the HelpLine to make a good faith report of an issue. However, please be aware that making a false report could result in discipline.

# Compliance Policies

---

- Northwell Health has a number of policies that support the operation of our compliance program. These policies cover several topics include, but are not limited to, privacy, security, coding, billing, identifying risk areas, responding to compliance issues promptly as identified in the course of audits, internal reviews, and Compliance HelpLine inquiries.
- Please see a complete listing of our policies on the Annual Mandatory Education and Orientation Materials main page under “Compliance Policies”. If you have questions about any of the policies, please contact your supervisor or manager, the Office of Corporate Compliance at (516) 465-8097, the Compliance Director assigned to your facility, or the Chief Corporate Compliance Officer.

# Other Important Northwell Health Contacts Discussed In These Materials

Group	Phone Number	Email or Web Address
Corporate Security	(516) 321-6900	<a href="https://intranet.northshorelij.com/NSLIJ/departments/NetworkEmerMgmt/Pages/Corporate%20Security%20and%20Emergency%20Management.aspx">https://intranet.northshorelij.com/NSLIJ/departments/NetworkEmerMgmt/Pages/Corporate%20Security%20and%20Emergency%20Management.aspx</a>
Employee Health Services	(516) 562-4697	<a href="mailto:EHS@northwell.edu">EHS@northwell.edu</a>
Coding		<a href="mailto:codingreimbursement@northwell.edu">codingreimbursement@northwell.edu</a>
Legal Affairs	(516) 321-6650	
Institutional Review Board	(516) 562-3100	<a href="http://www.feinsteininstitute.org/professional/resources-for-investigators/administrative-services/human-research-protection-program/">http://www.feinsteininstitute.org/professional/resources-for-investigators/administrative-services/human-research-protection-program/</a>
IS Service Desk	(516, 718, 631) 470-7272	<a href="https://intranet.northshorelij.com/NSLIJ/departments/IS/Pages/Home.aspx">https://intranet.northshorelij.com/NSLIJ/departments/IS/Pages/Home.aspx</a>
Procurement	(516) 396-6051	<a href="mailto:ProcurementCS@northwell.edu">ProcurementCS@northwell.edu</a>
Public Relations Department	(516) 321-6701	<a href="https://intranet.northshorelij.com/NSLIJ/departments/webservices/Pages/PublicRelations.aspx">https://intranet.northshorelij.com/NSLIJ/departments/webservices/Pages/PublicRelations.aspx</a>