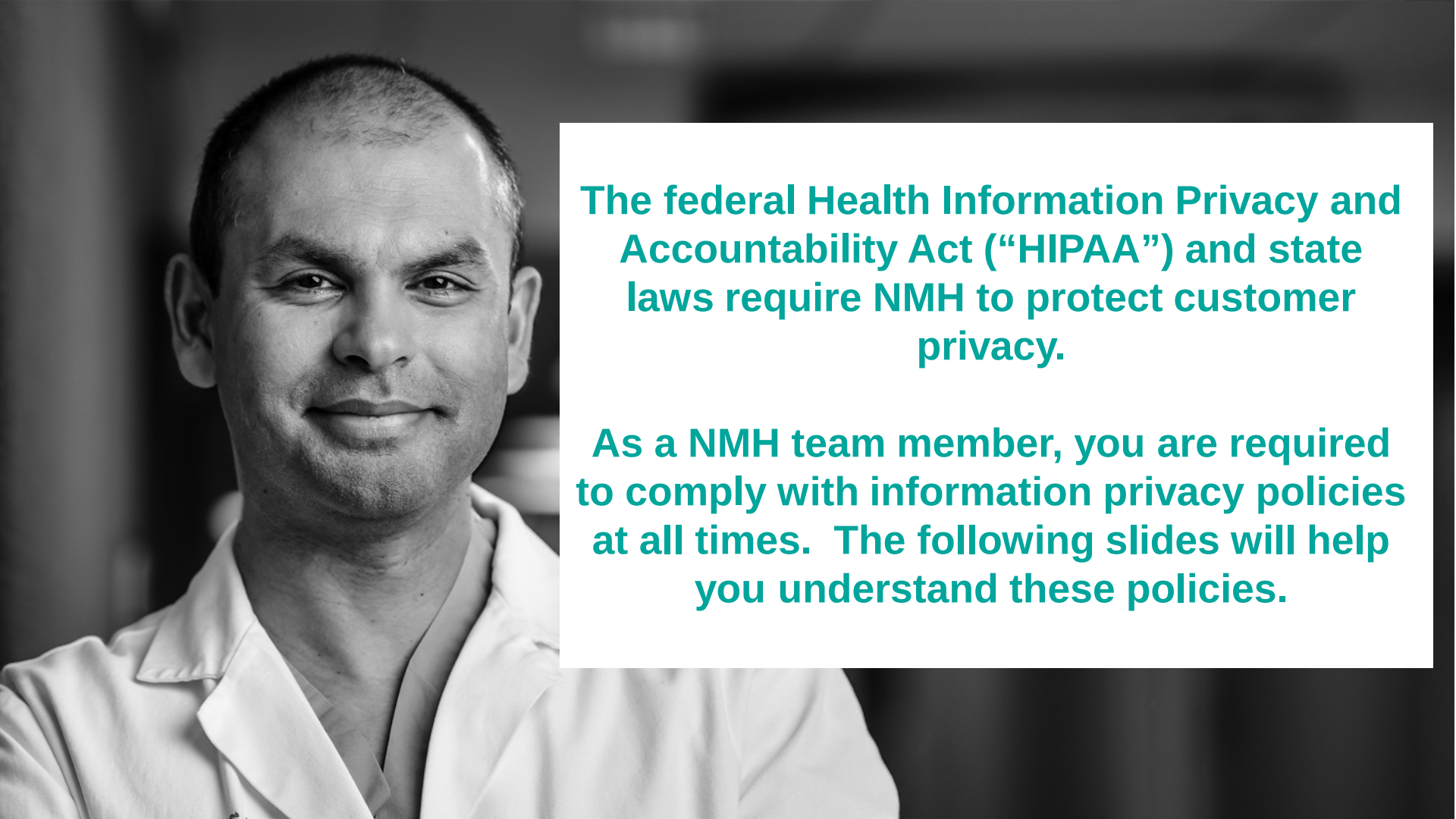
NORTH MEMORIAL HEALTH

2018 Information Privacy Training

As a NMH team member, you are responsible for protecting the privacy and security of customer information.

This module helps you understand your responsibilities related to information privacy.

NORTH MEMORIAL HEALTH



The federal Health Information Privacy and Accountability Act (“HIPAA”) and state laws require NMH to protect customer privacy.

As a NMH team member, you are required to comply with information privacy policies at all times. The following slides will help you understand these policies.

Protected Health Information

NMH must protect our customer's Protected Health Information (PHI). Not only is this a compliance obligation, it is also a requirement for providing unmatched customer service.

PHI is customer information that:

- Identifies or could reasonably be used to identify the customer; and
- Relates to the customer's health, health services received, or payment for those services.

NORTH MEMORIAL HEALTH

Minimum Necessary

When doing your job, you may only access the minimum amount of PHI necessary for you to accomplish your work.

- **This is known as the “minimum necessary rule.”**
- **NMH privacy policies prohibit you from viewing any information that is not required for you to complete your job tasks.**

NORTH
MEMORIAL HEALTH

Disclosure of PHI

- **Similarly, disclosures of information outside of the organization should be limited to the minimum amount of PHI necessary to fulfill the request.**

- **However, minimum necessary does not apply to disclosures made for treatment purposes.**

NORTH
MEMORIAL HEALTH

Disclosure of PHI

- **Most disclosures that are for purposes other than treatment, payment or health care operations require customer authorization.**
- NMH privacy policies explain when disclosures may be made without authorization. Examples include:
    - Reporting child abuse/neglect to child protective services.
    - Responding to inquires from health oversight agencies, such as the Centers for Medicare and Medicaid Services (CMS) or the MN Department of Health.
- NMH privacy policies provide additional information about appropriate disclosures. When in doubt, do not disclose PHI outside of NMH without consulting the Privacy Department.

NORTH
MEMORIAL HEALTH

You must take the following steps to protect PHI:

- Do not discuss PHI in public areas.
- Do not leave written PHI unattended or in plain view.
- If visitors are present when interacting with a customer, you should ask the customer if he/she would prefer privacy before discussing PHI.

NORTH
MEMORIAL HEALTH

You must take the following steps to protect PHI:

- Do not leave PHI in voicemail messages.
- When taking a telephone call, verify the identify of the caller before providing any PHI. Only provide PHI to authorized individuals.
- If faxing PHI, always use a cover sheet to protect any PHI on the other pages of the fax.
- PHI can be sent internally via email. No PHI (e.g., patient name or MRN) should be in the subject line of the email.
- Any PHI emailed outside of NMH must be sent secure and encrypted.

NORTH
MEMORIAL HEALTH

You must take the following steps to protect PHI:

- Double check patient identifiers on all paperwork, such as discharge summaries and after visit summaries before handing paper to customers. This will prevent PHI from being given to the wrong customer.
- All paper containing PHI must be disposed of in confidential destruction bins (Shred-It). Keeping discarded PHI in a box near your work station is prohibited.

NORTH
MEMORIAL HEALTH

Cell Phones and Social Media

- **Never take customer photos or transmit PHI over personal cell phones/devices.**

- **Never post North Memorial business or PHI online.**

The NMH Social Media Policy provides guidance for social media use. The Social Media user guide can be found on the Compliance intranet webpage.

NORTH MEMORIAL HEALTH

HIPAA Privacy and Epic Use

NMH team members who use Epic must follow privacy policies to ensure the privacy of customer information.

Curiosity is NEVER an appropriate reason to look at customer PHI.

- You must have a business purpose for accessing any patient record.
- Only access the minimum necessary PHI needed to complete your work.
- The next slides provides examples of Epic use that is prohibited.

NORTH
MEMORIAL HEALTH

HIPAA Privacy and Epic Use

NMH privacy policies prohibit you from viewing:

- Census reports/customer records from units where you are not assigned.
- Records of family members, friends, co-workers, etc. unless required to do your job.
- Records of customers that you hear about in the news.
- Pages or portions of the Epic record that you do not need to access in order to complete your work.

NORTH
MEMORIAL HEALTH

Epic “Break-the-Glass”

- NMH uses Break the Glass functions in Epic as an added level of information security to certain health records that require additional privacy protections.
- If you get a Break the Glass notice, complete the prompts within Epic to access the record and do your job.
- If you get a Break the Glass notice, and you do not have a job related reason for viewing the record, close the record immediately.
- Privacy Department staff routinely monitor Break the Glass access.

NORTH
MEMORIAL HEALTH

Epic access to your own health record

- NMH privacy policies do not prohibit staff from using Epic to view their own health record.
  - **However,** you are **strongly encouraged** to use MyChart to access your records.
  - MyChart is the Epic portal designed for use by all customers, including NMH employees who are also customers of NMH.
  - You may also access your health records by following the Health Information Management medical record access process.
- Team members are prohibited from documenting in or modifying their own health records in any way.

NORTH MEMORIAL HEALTH

Epic access to family records is prohibited.

Team members are prohibited from viewing the Epic records of their children (regardless of age), spouse, or other family members.

Employees who access the Epic records of family members are subject to investigation and disciplinary action.

NORTH
MEMORIAL HEALTH

Customer’s Privacy Rights

Customers have the right to:

- Access their health records.
- Request confidential communications and restrictions on their health records.
- Request amendments to their records.
- Request a list of certain disclosures of their health records.

Release of information requests and other requests related to health records should be directed to the Health Information Management department.

NORTH MEMORIAL HEALTH

Business Associates

- NMH has contracts with many vendors and business partners that perform functions or activities on behalf of NMH that involve the use or disclosure of PHI.
- These partners are known as Business Associates under HIPAA.
- Prior to disclosing any PHI to a Business Associate, NMH must have a signed contract and a business associate agreement.
- All questions regarding Business Associate Agreements should be referred to the Privacy Department.

NORTH
MEMORIAL HEALTH

Privacy Audits

- **All team members are subject to random and focused privacy audits.**
  - If Privacy identifies Epic access that was not for a business purpose or was not limited to the minimum necessary, Privacy will contact the team member's manager and request follow-up.
  - Privacy policy violations are subject to disciplinary action in accordance with HR policies.
- **NMH must report all confirmed privacy breaches to the Office for Civil Rights, which oversees HIPAA enforcement.**

NORTH MEMORIAL HEALTH

Privacy Investigations

- All reports of privacy non-compliance are investigated by the Privacy Department.
- Reports may be made by any team member, customer, or family member.
- Reports may be made to the Privacy Officer.

NORTH MEMORIAL HEALTH

Compliance Contacts

Kelsey Brodsho, *Chief Compliance Officer*
Kelsey.Brodsho@northmemorial.com
compliance@northmemorial.com
763.581.0976

Deb Contreras, *Privacy Officer*
Deb.contreras@northmemorial.com
privacy@northmemorial.com
763.581.4437

Mike Sweet, *Data Security Officer*
Mike.sweet@northmemorial.com
datasecurity@northmemorial.com
763.581.2503

NORTH
MEMORIAL HEALTH