HIPAA 101

The Health Insurance Portability and Accountability Act (HIPAA) protects patient privacy.
- HIPAA is a Federal law that includes:
  - criminal (i.e. prison terms); and
  - civil (i.e. monetary fines) penalties.

As a member of DMC’s workforce, **YOU** are responsible for utilizing safeguards and complying with DMC’s policies to uphold the confidentiality of all Protected Health Information (PHI).

DMC policies also describe NYS laws that protect patient privacy.
What is Protected?

**Protected Health Information** is any information that can be linked to a specific individual about:

- health status;
- provision of care; or
- payment

1. Names
2. Geographical identifiers
3. Dates directly related to an individual
4. Phone numbers
5. Fax numbers
6. **Email** addresses
7. **Social Security numbers**
8. Medical record numbers
9. **Health insurance** beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers license plate numbers;
13. Device identifiers/ serial numbers;
14. Web (URLs)
15. Internet Protocol (IP) address #
16. **Biometric** identifiers including fingerprints
17. Full face photographic images
18. Any other unique identifying number, characteristic, or code.
Privacy is Priceless…

Once a breach of PHI occurs, privacy can never be restored!

Always avoid removing PHI from DMC’s premises unless absolutely necessary.

Appropriate safeguards must be in place for all PHI in your possession or control.

Onsite
Or
Offsite
Keep PHI out of sight and out of earshot!

- Professional conversations should never take place in public areas
- Semi-private rooms: use reasonable precautions (lower your voice)
- Voice messages/Intercom announcements: No info specific to patient’s service/conditions
- Monitors should be facing away from public view
- Sign-In Logs should have Name, Date & Time only
- Secure Patient Charts/ Interoffice mail
- NEVER Leave PHI Unattended
- Check with patient or review his/her chart for consent before discussing care with visitors, including stating medications out loud
Safeguards

Keep Databases / Workstations on lock!

- NEVER share passwords
- Exit / log-out before leaving a workstation
- Use privacy screens on monitors when necessary
- Restrict access to minimum necessary
Properly dispose of PHI!

- NEVER dispose PHI in trash cans – Use secure bins or shredders. All printed materials and copies including faxes, emails, or reports containing PHI must be shredded or placed in secure bins designated for shredding.

- Diskettes and CDs must also be disposed of properly; destroyed or placed in designated bins for shredding.
- Properly and permanently delete PHI from electronic storage before disposal
- Follow role change / termination procedures to ensure PHI is returned when appropriate
IT Security - Downloading, Copying, Removing

- Never send PHI via personal email – Office Outlook must be used
- Encrypt PHI whenever possible – but always encrypt when transmitting via internet
- Patient images taken with mobile device must be uploaded and immediately deleted before going offsite
- USB drives/ portable devices containing PHI may never be taken off-site or used for long term/ permanent storage unless they meet DMC encryption standards
  - Portable devices include laptops, notebooks, hand-held computers, tablets (iPads), Personal Digital Assistants, smartphones and USB drives
Special Categories

- HIV
- Mental Health
- Alcohol/Substance Abuse

Treatment related to these categories is especially sensitive.

The regulations provide special privacy requirements when dealing with this type of information.
Top Violations

The #1 reported violation: Impermissible uses and disclosures

- Discussing or leaving PHI in public places
- Disposing of PHI in regular trash bins
- Lost or stolen portable devices (laptops, thumb drives) containing PHI
- Failure to obtain necessary patient authorization, including discussing care in the presence of visitors without asking permission from the patient first
- Snooping into patient files

AVOID A VIOLATION!

ALWAYS BE SURE THAT APPROPRIATE SAFEGUARDS ARE IN PLACE
When In Doubt…

Review policies & procedures
www.downstate.edu/hipaa

Policies accessible via sidebar:

“HIPAA Privacy Policies”

<table>
<thead>
<tr>
<th>HIPAA Privacy Policies</th>
<th>POLICY PDF</th>
<th>FORM / ATTACHMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accounting of Disclosure</td>
<td>Patient Request Accounting of Disclosure Form</td>
<td>Accounting of Disclosure HIPAA Policies Template</td>
</tr>
<tr>
<td>Alcohol and Substance Abuse Information (Special Category)*</td>
<td></td>
<td>Alcohol and Substance Abuse HIPAA Policies Template</td>
</tr>
<tr>
<td>Business Associate Agreements</td>
<td></td>
<td>Business Associate Agreement Template</td>
</tr>
<tr>
<td>Compliance and Enforcement</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compliance (&amp; HIPAA) Training</td>
<td></td>
<td>Course Requirement Matrix</td>
</tr>
<tr>
<td>Covered Entity Determination</td>
<td></td>
<td></td>
</tr>
<tr>
<td>De-Identification of Information</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Designated Record Set</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Facility Directory</td>
<td>Facility Directory Form</td>
<td></td>
</tr>
<tr>
<td>Faxed Patient Information</td>
<td>Fax Cover Page</td>
<td></td>
</tr>
<tr>
<td>fundraising Activities</td>
<td>fundraising Opt-Out Form</td>
<td></td>
</tr>
<tr>
<td>HIV Related Information (Special Category)*</td>
<td>NOP For HIV Info</td>
<td></td>
</tr>
<tr>
<td>Marketing Activities</td>
<td>Marketing Authorization Form</td>
<td></td>
</tr>
</tbody>
</table>
Lost or Stolen PHI

IMMEDIATELY REPORT!

If you suspect that PHI in any form has been lost or stolen, report to:

- Immediate Supervisor
- Office of Compliance & Audit Services
- Confidential Compliance Hotline: 877-349-SUNY
- OR Web-based Reporting: “Compliance Line” link located at bottom of www.downstate.edu
If you have questions about the safeguarding of PHI, or how to properly dispose of PHI, **ASK!**