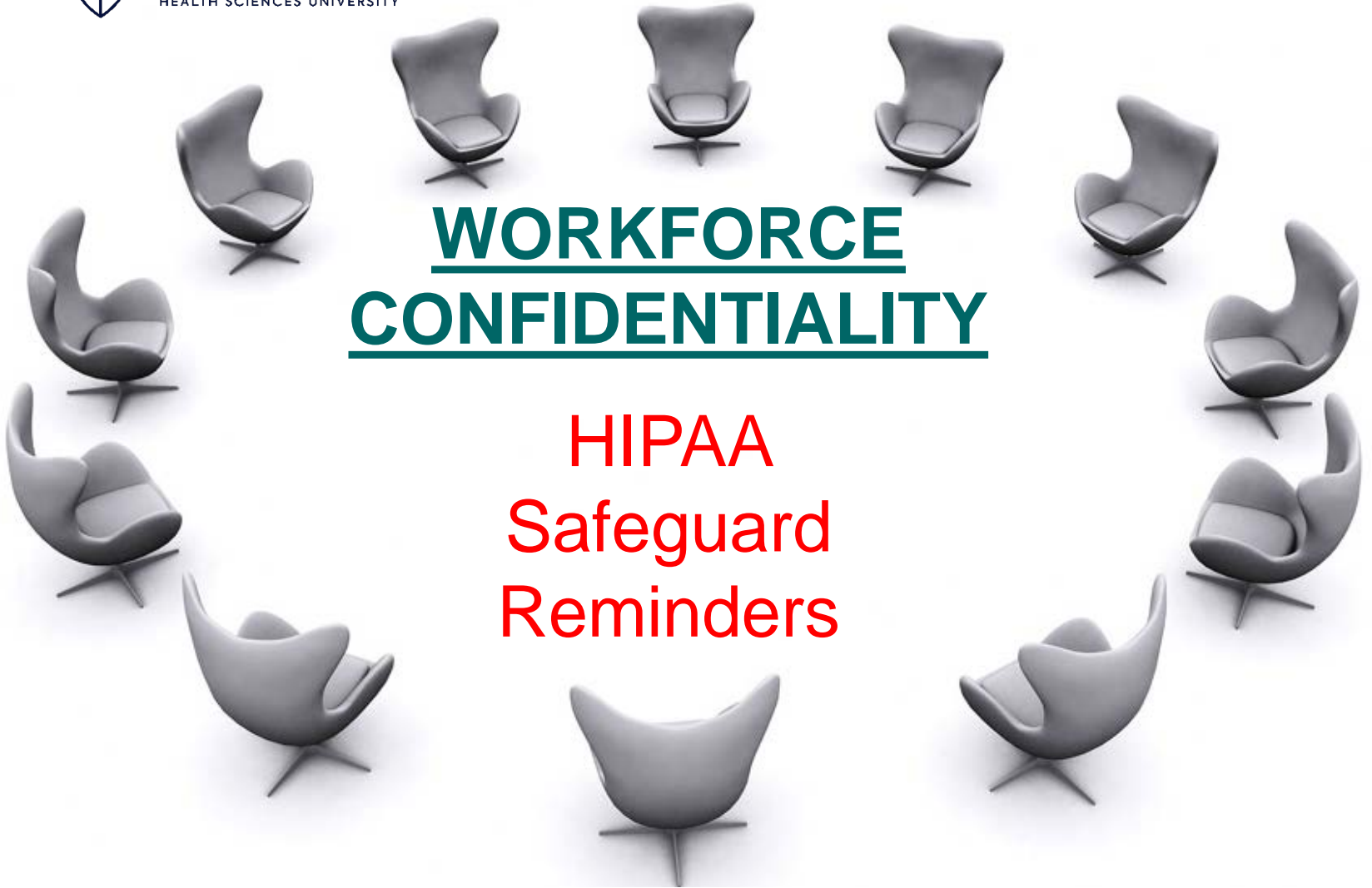




DOWNSTATE
HEALTH SCIENCES UNIVERSITY

WORKFORCE CONFIDENTIALITY

HIPAA
Safeguard
Reminders



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 Downstate's workforce, YOU are responsible for utilizing safeguards and complying with Downstate's policies to uphold the confidentiality of all Protected Health Information (PHI).

Downstate 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 Downstate's premises unless absolutely necessary.

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

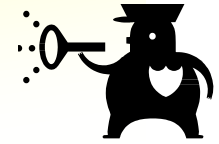
Onsite

Or

Offsite



...Safeguards

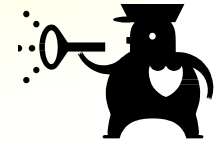


Keep PHI out of sight and out of earshot!



- 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**
- **Verify a patient's name before handing over documents (i.e. Rx / Discharge Info. / Bill or Receipt)**

...Safeguards

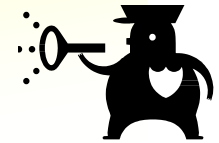


Keep Databases / Workstations on lock!



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

...Safeguards

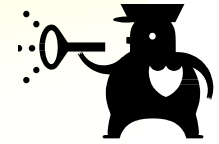


Properly dispose of PHI!

- 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



...Safeguards



IT Security - Downloading, Copying, Removing

- Never send PHI via personal email – Outlook must be used
- **Encrypt PHI whenever possible – but always encrypt when transmitting via internet**
 - **Manually encrypt confidential emails by typing 'Confidential' in the subject heading**
- 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 Downstate encryption standards
 - Portable devices include laptops, notebooks, hand-held computers, tablets (iPads), Personal Digital Assistants, smart phones 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

CAUTION

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!

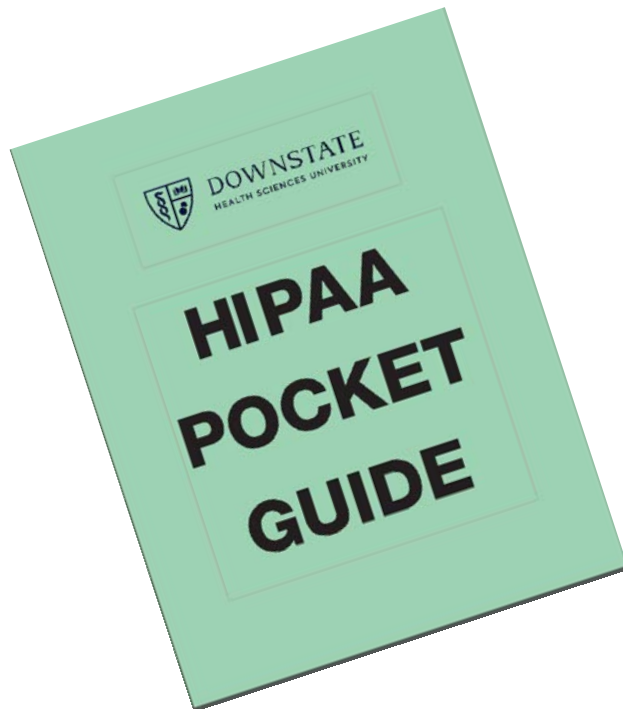
ALWAYS BE SURE THAT APPROPRIATE SAFEGUARDS ARE IN PLACE

When In Doubt...

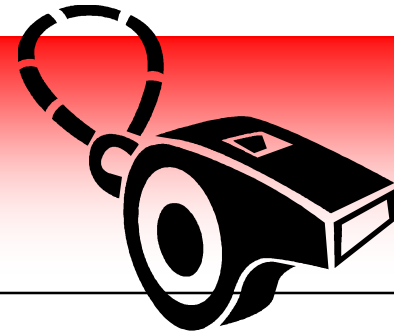


Downstate's HIPAA Privacy Policies are available on our website.

Downstate.edu -> Our Administration -> HIPAA



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**

Contact Us



If you have questions about the safeguarding of PHI, or how to properly dispose of PHI, **ASK!**

