HIPAA Implications in our High Tech World

August 24, 2018

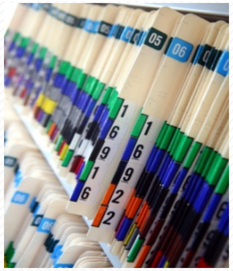
Office of Compliance & Audit Services

Agenda

- Summary of HIPAA Rule
- Device Controls
- Electronic Communications with Patients
  - Emails/ Texts
  - Patient Portal
- Patient Photos & Videos
- Social Media
- Cloud Computing
- Audit Trails
- Breach of PHI
- Compliance Line Reporting

HIPAA Privacy Rule Summary

- The Health Insurance Portability and Accountability Act (HIPAA) protects patient privacy in all forms:



Written

Oral

Electronic

- HIPAA is a Federal law that includes:
  - ✓ Criminal penalties (i.e. prison terms); and
  - ✓ Civil penalties (i.e. monetary fines).
- 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).

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*

** When using PHI for research or education, de- identify whenever possible!*

Common PHI Identifiers

PHI	Example
Name	Mr. B. Individual
Address	987 Main Street, Yourtown, KY 45678
Telephone #	(432) 567-0000
Date of birth	12/29/74
SSN	000-00-0000
Email address	bindiv@mail.com
MRN	#3214325879
Account #	#7493875949383
Genetic information	Huntington's Disease
Photographs	

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.

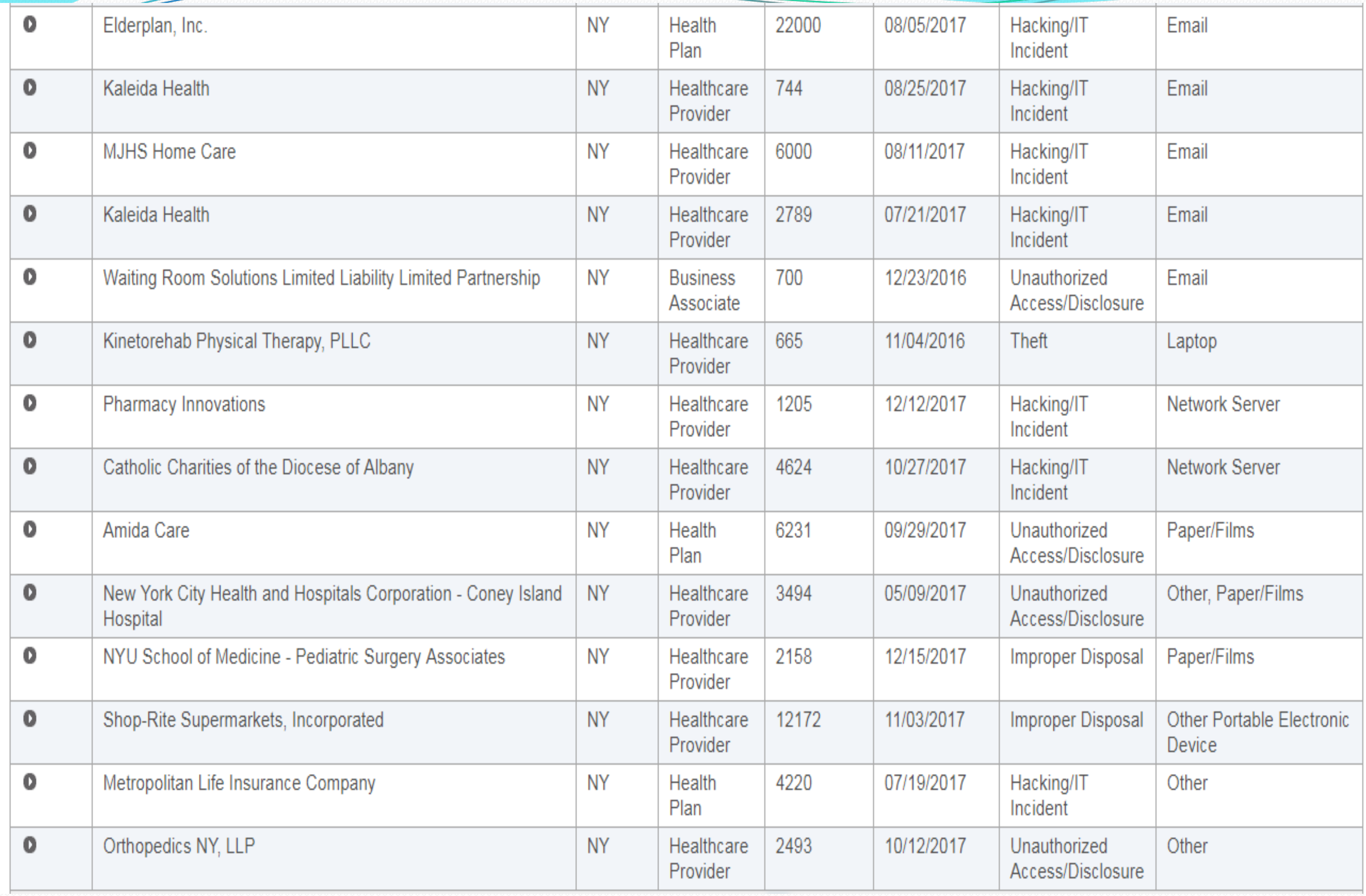
Top Violations

- Impermissible uses and disclosures of protected health information;
- Lack of safeguards of protected health information;
- Lack of patient access to their protected health information;
- Lack of administrative safeguards of electronic protected health information.
- Use or disclosure of more than the minimum necessary protected health information;

AVOID A VIOLATION!

ALWAYS BE SURE THAT APPROPRIATE SAFEGUARDS ARE IN PLACE

List of HIPAA Breaches in NY from Public Website



●	Elderplan, Inc.	NY	Health Plan	22000	08/05/2017	Hacking/IT Incident	Email
●	Kaleida Health	NY	Healthcare Provider	744	08/25/2017	Hacking/IT Incident	Email
●	MJHS Home Care	NY	Healthcare Provider	6000	08/11/2017	Hacking/IT Incident	Email
●	Kaleida Health	NY	Healthcare Provider	2789	07/21/2017	Hacking/IT Incident	Email
●	Waiting Room Solutions Limited Liability Limited Partnership	NY	Business Associate	700	12/23/2016	Unauthorized Access/Disclosure	Email
●	Kinetorehab Physical Therapy, PLLC	NY	Healthcare Provider	665	11/04/2016	Theft	Laptop
●	Pharmacy Innovations	NY	Healthcare Provider	1205	12/12/2017	Hacking/IT Incident	Network Server
●	Catholic Charities of the Diocese of Albany	NY	Healthcare Provider	4624	10/27/2017	Hacking/IT Incident	Network Server
●	Amida Care	NY	Health Plan	6231	09/29/2017	Unauthorized Access/Disclosure	Paper/Films
●	New York City Health and Hospitals Corporation - Coney Island Hospital	NY	Healthcare Provider	3494	05/09/2017	Unauthorized Access/Disclosure	Other, Paper/Films
●	NYU School of Medicine - Pediatric Surgery Associates	NY	Healthcare Provider	2158	12/15/2017	Improper Disposal	Paper/Films
●	Shop-Rite Supermarkets, Incorporated	NY	Healthcare Provider	12172	11/03/2017	Improper Disposal	Other Portable Electronic Device
●	Metropolitan Life Insurance Company	NY	Health Plan	4220	07/19/2017	Hacking/IT Incident	Other
●	Orthopedics NY, LLP	NY	Healthcare Provider	2493	10/12/2017	Unauthorized Access/Disclosure	Other

Reasonable Safeguards

- 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, whether on- site or off- site.

<u>Keep PHI Out of Sight and Out of Earshot</u>!

- 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
- NEVER Leave PHI Unattended
- Check with patient or review his/her chart for consent before discussing care with visitors, including stating medications out loud

Reasonable Safeguards: Device Controls

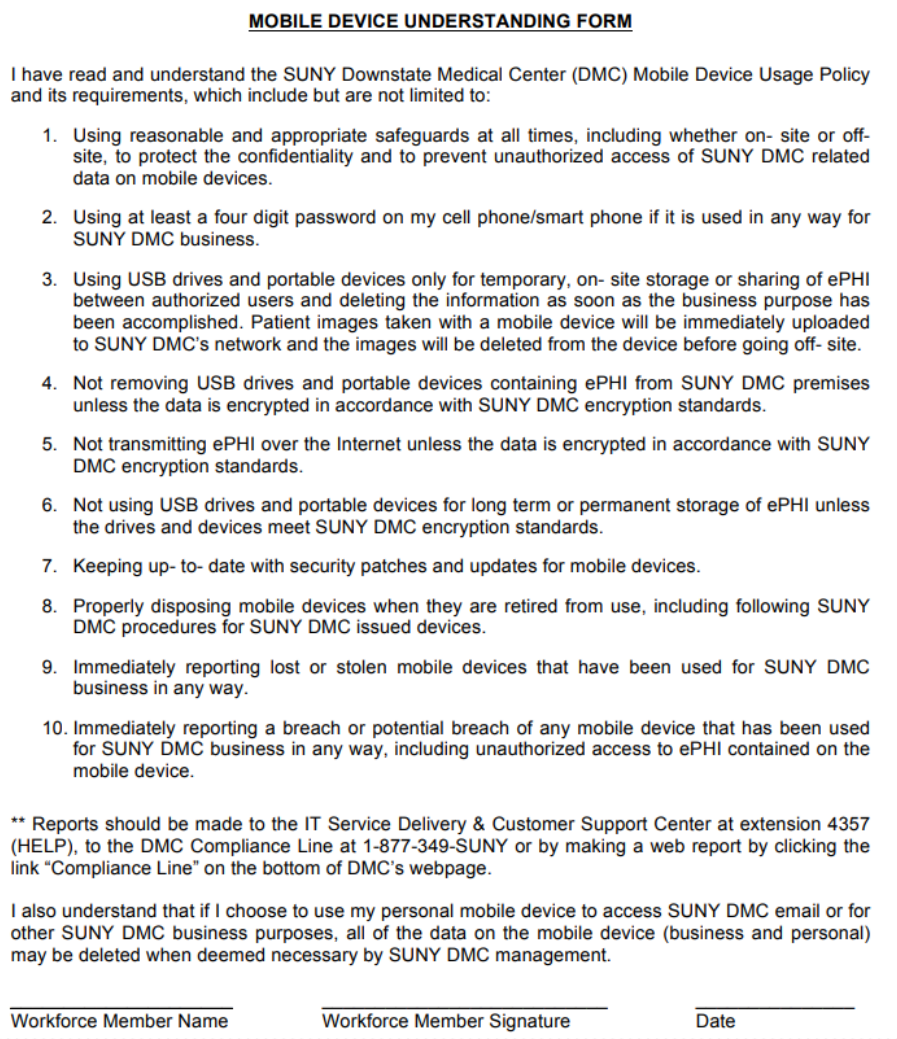
- Databases/ Workstations
- ✓ Unique ID's- do not share with residents/ fellows/ students!
- ✓ Passwords- do not place in accessible area

- Keep bags containing portable devices with you at all times
- Never leave devices in unsecured vehicles
- Never leave devices powered up, accessible and unattended in your home if others live with you
- Dispose CD's/ thumb drives in shredder or permanently delete files

- Mobile devices, laptops, USB drives
- ✓ ENCRYPT, ENCRYPT, ENCRYPT!
- ✓ If not, do NOT take off- site and use only for temporary storage of information

DMC Policy: Mobile Device Usage

- Located at: http://is.downstate.edu/policies/index.html



MOBILE DEVICE UNDERSTANDING FORM

I have read and understand the SUNY Downstate Medical Center (DMC) Mobile Device Usage Policy and its requirements, which include but are not limited to:

1. Using reasonable and appropriate safeguards at all times, including whether on- site or off-site, to protect the confidentiality and to prevent unauthorized access of SUNY DMC related data on mobile devices.
2. Using at least a four digit password on my cell phone/smart phone if it is used in any way for SUNY DMC business.
3. Using USB drives and portable devices only for temporary, on- site storage or sharing of ePHI between authorized users and deleting the information as soon as the business purpose has been accomplished. Patient images taken with a mobile device will be immediately uploaded to SUNY DMC's network and the images will be deleted from the device before going off- site.
4. Not removing USB drives and portable devices containing ePHI from SUNY DMC premises unless the data is encrypted in accordance with SUNY DMC encryption standards.
5. Not transmitting ePHI over the Internet unless the data is encrypted in accordance with SUNY DMC encryption standards.
6. Not using USB drives and portable devices for long term or permanent storage of ePHI unless the drives and devices meet SUNY DMC encryption standards.
7. Keeping up- to- date with security patches and updates for mobile devices.
8. Properly disposing mobile devices when they are retired from use, including following SUNY DMC procedures for SUNY DMC issued devices.
9. Immediately reporting lost or stolen mobile devices that have been used for SUNY DMC business in any way.
10. Immediately reporting a breach or potential breach of any mobile device that has been used for SUNY DMC business in any way, including unauthorized access to ePHI contained on the mobile device.

** Reports should be made to the IT Service Delivery & Customer Support Center at extension 4357 (HELP), to the DMC Compliance Line at 1-877-349-SUNY or by making a web report by clicking the link "Compliance Line" on the bottom of DMC's webpage.

I also understand that if I choose to use my personal mobile device to access SUNY DMC email or for other SUNY DMC business purposes, all of the data on the mobile device (business and personal) may be deleted when deemed necessary by SUNY DMC management.

____________________ ____________________ ____________
Workforce Member Name Workforce Member Signature Date

Recent OCR Settlements Related to Encryption

- University of Texas MD Anderson- June 2018
  - ✓ $4.3M
  - ✓ Theft of one unencrypted laptop from employee residence and loss of two unencrypted thumb drives
  - ✓ Exposed 33,500 patients

- CardioNet (remote mobile monitoring of patients)
  - ✓ $2.5M
  - ✓ Theft of one stolen laptop, insufficient policies on mobile device security
  - ✓ Exposed 1,391 patients

Electronic Communications with Patients

- Obtain authorization via approved consent form PRIOR to emailing patients

✓ Established relationship

✓ Literacy adequate for electronic communication

- Standard information should include:

✓ Provider full name & contact info

✓ Established response time

✓ Instructions for when response time not met

✓ Instructions for urgent communications/ emergencies

✓ Statement that patients may escalate to a phone call or visit at any time

✓ Statement that email is not a substitute for clinical eval

✓ Generic confidentiality statement

DMC Policy: Electronic Communications

- Located at: http://www.downstate.edu/regulatory/pdf/policies/HIS-11.pdf
- NEVER communicate with patients using personal email accounts
- Use encryption: Insert “Confidential” in Subject line of DMC’s Outlook email system to auto encrypt
- Text patients/ other providers ONLY with DMC approved texting service- do not include specific health info
- Use Patient Portal- secure message service is encrypted, clinically relevant messages can be made part of the EHR
- Follow appropriate guidelines for communicating ethically and responsibly including avoiding anger/ sarcasm in messages.

Electronic Communications: Departmental Procedure

- Establish response time- frames and work- flows

- Permitted communications:

✓ Prescription renewals
✓ Non- urgent medical advice
✓ Test results, based upon professional judgment
✓ Scheduling/ canceling/ rescheduling appointments
✓ Clinic/ provider changes

- Prohibited communications:

✓ HIV info
✓ Alcohol and substance abuse info
✓ Genetic testing
✓ Workers comp injuries
✓ Confusing/ abnormal test results
✓ New diagnoses
✓ Bad news
✓ Info deemed urgent in provider's professional opinion
✓ Info pertaining to legal liability

I HATE TO TELL YOU BUT...
How to give bad news to your clients

- NEVER communicate electronically for medical emergencies

Patient Photos & Videos

- Provider may not use/ disclose PHI except if a) permitted under HIPAA; b) authorized by patient.
- Providers may not allow members of media/ film crews into treatment areas or other areas where PHI is accessible in written, electronic or oral form.
- Not sufficient to require media to mask identities of patients (blurring, voice alteration) because HIPAA does not allow access to patients' PHI without patient authorization.
- Reasonable safeguards to protect against impermissible disclosures when authorization has been obtained.

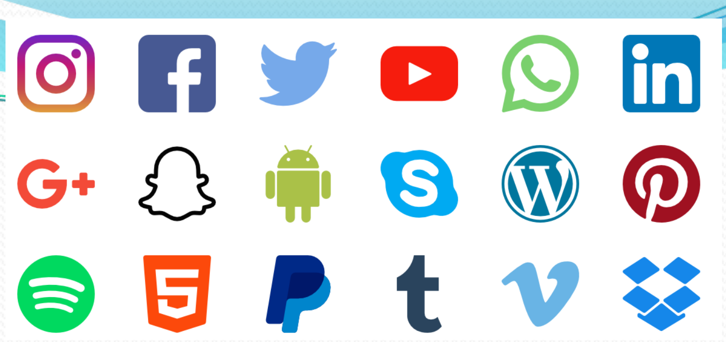
UHB Policy on Photography

- Located on Intranet: http://www.downstate.edu/regulatory/pdf/policies/CONS-07.pdf
- No specific authorization required for the purpose of identification, diagnosis, treatment and internal education- General Consent for Treatment is sufficient;
- Documenting/ treating abuse/ neglect of a minor does not require consent of parent but may be appropriate to seek minor/ parent agreement to photography
- All other uses require specific authorization
  - ✓ Research protocol: IRB approval
  - ✓ Media requests: Handle through Communications Office
- Be cognizant of patients/ staff in background
  - ✓ Patient may refuse at any time;
  - ✓ Physicians/ nurses have authority to cease photography/ filming if compromises patient care, patient/ staff privacy or safe/ effective hospital operations
- If taking photo/ video from mobile device, upload to hospital server/ system prior to going off- site and delete from device

DMC Policy on Media Authorizations

- Media Authorization Form located at: http://www.downstate.edu/ia/policies.html
- Use for statement/ interviews, photographs, illustrations, videos, audio recordings
- Purposes: news media, professional journals, publication, broadcast, social media/ Internet, symposiums/ poster sessions, events.
- Requires disclosure whether DMC will receive direct or indirect remuneration.
- Not required if fully de- identify the data.

Social Media



MAJOR RISK AREA

- Be mindful of sharing information!
  - Never include patient specific information- potential for inadvertent privacy violations
  - Never post pictures of sensitive areas
  - Patients/ workplace/ other associates can inadvertently be seen in background
  - Never provide medical advice in non- clinical setting
  - Be wary of unintentionally endorsing or advertising a product
  - Be careful of other discriminatory or offensive comments related to job responsibilities
  - Online patient reviews can be tricky!

DMC Policy: Social Media

- Located at: http://www.downstate.edu/policy/pdf/final-social-media-policy-11-10-17.pdf
- Institutional representation on social media sites must be authorized by DMC
- Numerous laws: HIPAA, FERPA, copyright/ trademark/ intellectual property, FOIL
- Written consent to use recordings, photos, images, videos, slideshows, artwork, advertisements
- Compliant with data protection safeguards
- Policy Excerpt: "In order to comply with HIPAA, social media sites must not be used when communicating about an issue involving a specific patient. Patient information may not be posted, even if it has been 'de- identified'. It is often possible to identify patients even if their names or other identifying information are not included, particularly to the patients themselves and their friends or family members."

Cloud Computing

- Considered “business associate” under HIPAA rules
- Requires execution of a Business Associate Agreement (BAA)- Coordinated by DMC Procurement Office
- Service level agreement should consider:

✓ Backup/ data recovery
✓ Retention time- frames
✓ Authentication/ user identification protocols
✓ Internal controls for administrative access
✓ Server locations outside of the US

- Do NOT use a platform/ service for PHI/ confidential materials if it has not been approved by DMC!

DMC Policy: Outlook OneDrive

- OneDrive currently available via Portal and mobile device
- Storage of files within OneDrive is secure and covered by DMC’s BAA with Microsoft
- Problem occurs when users download the files to non- Downstate computers/ devices
- Solution: Work on files only within OneDrive; do not download. Best not to use for sensitive information.

Audit Trails

- HIPAA Security Rule requires organizations to perform security audits: to implement mechanisms that record and examine activity in information systems and to regularly review
- Also required under HITECH, Meaningful Use, TJC, E-discovery*

✓ Detects unauthorized access to patient information- theft of patient data, snooping into records

✓ Provides evidence during investigations

✓ Tracks disclosures of PHI

✓ Responds to patient privacy concerns

✓ Detects new threats and intrusion attempts

- Audit logs typically include: User name, patient name, screens accessed, view only vs modification, date of access

*American Health Information Management Association (AHIMA) Body of Knowledge- Privacy & Security Audits of Electronic Health Information 2014

Recent OCR Settlements Related to Audit Trails

- Memorial Healthcare System (Florida)
- Fined $5.5M
- Former employee’s login credentials were never terminated and the employee accessed information for over a year (80,000 patients)
- Guilty due to lack of timely termination procedures and lack of information system activity review

DMC Process for Audit Log Review

- Currently audits access of patient records that are employees of DMC
- IT working on logs to review:

✓ Access of same last name

✓ VIP patient records

✓ Access of records with no activity after 120 days

✓ Inappropriate access across departments/ roles/ rights

✓ Records with sensitive information (STAR, HEAT, Mental Health Outpatient)

✓ Access of minors being treated for pregnancy or sexually transmitted diseases

Breach of PHI

The unauthorized:

- Access
- Use
- Disclosure

Examples:

- Wrong or unencrypted email
- Laptop or flash drive lost or stolen
- Improper disposal of equipment
- Accessing PHI of others “out of curiosity”

Breach Notification

- Knowledge of a breach means it has been “discovered” by someone in the organization.
- Requires risk assessment to determine if probability of PHI compromise is low.

✓ Nature/ extent of PHI involved

✓ The unauthorized person who used/ received the PHI

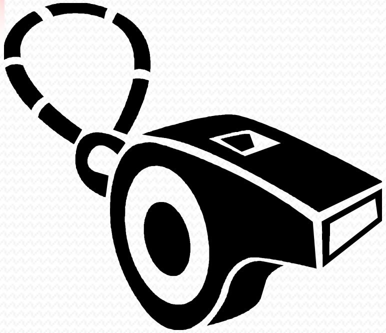
✓ Whether PHI was actually acquired/ viewed

✓ Extent to which risk has been mitigated

- This starts the clock ticking for the breach notification time period.
- Report actual or suspected breaches
- **Timely reporting is vital!**

We must report breaches to the individual **within 60-calendar days** of discovery, unless law enforcement requests a delay.

Compliance Line Reporting



IMMEDIATELY REPORT!

If you become aware of a breach of protected health information or other HIPAA violation, it is up to you to report it!

- 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**

Questions?