The Carle Foundation and Affiliates HIPAA Privacy and Security Quick Reference Guide (June, 2020)

1. What is HIPAA?
Privacy and Security laws such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA) require each individual at Carle to protect all medical and/or billing information containing patient identifiers. HIPAA privacy is about how we access, use and disclose protected health information.

2. How is health information protected?
The Privacy Rule governs the use and disclosure of "Protected Health Information" (PHI). PHI is any medical information in combination with any one of 18 patient identifiers. (Some common identifiers are: Name, address, date of birth, MRN, or any other unique identifying number, fingerprints, full face or other unique photographic images, etc.) Under the HIPAA Privacy Rule, PHI includes past, present, and future medical information/identifiers.

- "Use" is internal – that is, the way the Carle staff access and/or share information amongst other Carle staff in order to provide services to our patients.
- "Disclosure" is external – that is, when Carle staff shares PHI with others outside the Carle organization. Disclosure may be appropriate; however, when disclosure is not appropriate, it is a breach of the privacy laws.

3. Does the Privacy Rule allow us to use and disclose PHI?
Yes, the Privacy Rule allows Carle staff to access and use PHI without the patients' written approval or "authorization" for the purpose of treatment, obtaining payment for services, and for operations (things like audits or quality reviews). The state of Illinois specifically protects medical information related to HIV/AIDS, mental health, drug and alcohol abuse and genetics. Always be sure to check with your supervisor prior to disclosing this highly sensitive information.
Staff access to PHI is restricted to "need to know" and is *defined by job class*. This is called the "minimum necessary rule." Staff must restrict their access, use, and disclosure to the minimum amount of PHI necessary *to do their job*, and only when necessary to do their job.
Accessing and/or sharing information you do not need *to do your job* is a Carle policy violation and a Privacy Rule violation, and may lead to disciplinary action up to termination. If you hold a state license or certification, we may be required to report such violation to a state agency.

4. How do I know what the "minimum necessary" amount of information is?
To determine if you are requesting or providing the "minimum necessary" PHI, consider what information is needed to accomplish the intended purpose of your job, and whether the intended purpose is allowed under the Privacy Rule.

5. Otherwise…
If the use or disclosure is not for treatment, payment or allowable healthcare operations, we must have a patient's written authorization to use or disclose their PHI. There are specific situations that there may be a waiver of a patient's written authorization; however, this requires approval by a Privacy Board. Refer to Carle policy RES118- Uses and Disclosures of Protected Health Information for Research. You may contact the Research Institute at (217) 383-4366, or the Research Integrity Officer at (217) 902-5392 for questions concerning HIPAA waivers.

6. Privacy Rule - Reasonable Safeguards
The Privacy Rule requires Providers to use "reasonable safeguards" to protect the inappropriate or unauthorized use or disclosure of PHI.
*Some very important guidelines related to Carle's reasonable safeguards include:
Never access medical information, EMR or paper records, without a valid business need or necessary job function. (This includes yours, family members, coworkers, friends or "ex's" records.) Curiosity or concern is NEVER an excuse to access medical records. Obtain a "MyCarle" account for yourself and your family members. Encourage our patients to do the same.

- Always pause and verify documents are for the correct patient, and that all documents are for the same patient prior to handoff.
- Always verify phone numbers, fax numbers, addresses and email addresses prior to sending information.

- Prior to copying, scanning, emailing, or faxing utilizing our multifunction machines- clear the queue. Then, when you have completed your job, clear the queue again. (For example, press the "Home" button, or "Clear All" button) Doing this prevents misdirected documents.
- Use the dedicated recycle and locking bins & shredders to dispose of PHI.
- Keep charts/records/documents with patient information out of public view.
- Log off your computer and never share passwords, and always lock your desktop when stepping away.
- Lock file cabinets used to store PHI.
- Place PHI in an envelope, and use the blue mail jackets when sending items through the courier. Do not use the clear jackets.
- Restrict conversations about patients to private areas. Never discuss patient information outside of work.
- Be mindful of the volume of your voice in reception and other patient care areas.
- Another "reasonable safeguard" that we *must* utilize before we disclose PHI to anyone is to verify the identity of the person requesting the information. Refer to Carle Foundation Policy IM217, Verification of Identity and Authority of a Person Requesting Patient **Information** (PHI) for suggested methods to verify identity before disclosing PHI.

~ Resources~

Notice of Privacy Practices: Registration staff are responsible for providing the Notice of Privacy Practices to patients. The Notice of Privacy Practices, in addition to Carle policies and procedures, can be used as *your* resource to determine if a PHI *use* or *disclosure* is allowed. If something is not listed or referred to in the Notice, it is not allowed.

Patient Restriction Requests or Record Amendment Requests:
Refer patients to the Health Information Management Department (HIM), as the primary contact for all patient access requests. (E.g. requests for review of records, copies of records, requests for an amendment, restriction requests etc.)

Policies & Procedures:
The Carle Foundation has policies and procedures to address patient privacy rights created by HIPAA, and to instruct staff how to comply with the Privacy Rule in general. Refer to the Carle Intranet ("CLICK"); contact your leadership, or the Compliance Department for assistance with Carle's HIPAA-related policies.
Some common policies to reference (Not an exhaustive list.):

- Carle Standards of Conduct
- AD527 Authorization to Release Patient Information
- AD542 Personal Privacy, Confidentiality, Use and Disclosure of Patient Information
- IM207 Facsimile Machines, Telephones and Protected Health Information
- IM208 Encryption (This policy speaks to email encryption.)
- IM210 Release, Access and Disclosure of Medical Record Information
- IM211 Patient Confidentiality and Privacy- Minimum Necessary
- IM216 Disclosure of Protected Health Information to Family, Friends, or Others Directly Involved in the Patient's Care
- IM217 Verification of Identity and Authority of a Person Requesting Health Information. ("Call Backs"/I.D. checks)
- IM230 Electronic Communication of Protected Health Information

Patient Questions about access to their medical records or copies:
Refer patients or family members to the Health Information Management Department, Correspondence at 217-902-6500.

Patient Privacy Concerns or Complaints:
You may refer callers to the Compliance AlertLine number at 888-309-1566, Compliance Department, HIPAA Privacy Analyst at 217-902-5393. If more convenient for the patient, please document the patient's concerns, obtain any misdirected documents, and complete a HIPAA Incident Report.

HIPAA Incidents are reported via the HIPAA Incident Report Form, found on "CLICK" in the Compliance Department Links. An Accounting of Disclosure Form must also be filled out in conjunction with a HIPAA Incident Report Form. To ensure you are using the most up to date form, always go to the department page on "CLICK". Offer to send the patient a self-addressed, stamped envelope to return any documents to Carle. Note on the envelope, "Compliance, FA-CORP".

Staff, Volunteer, and other Carle Workforce Concerns or Complaints:
Relay any concern or complaint via our Ethics and Compliance AlertLine via phone at 1-888-309-1566 or the web link: https://Carle.alertline.com. The AlertLine allows concerns to be addressed anonymously. There is never any retaliation for reporting a concern or complaint. This reporting mechanism may be anonymous.

SECURITY TIPS:

- Promptly report suspected or known IT security incidents to the IT Help Desk at (217) 383-4357, and your supervisor. Never open emails that are suspicious or click on unfamiliar links within emails. This includes reporting a suspected computer virus.
- Guard against malicious software by downloading only Carle authorized software on to Carle IT equipment (e.g. use caution in downloading from the internet or saving document attachments in email to the network from unfamiliar or un-trusted sources, which can introduce viruses to our network). Always ask prior to downloading anything. Never allow browsers to save passwords.
- Be wary of "shoulder surfers" – others watching your keystrokes as you log in.
- Always safeguard your user IDs and passwords. Never share them with anyone and never write them down where someone may have access to them (e.g. DO NOT tape them to a computer monitor or inside a desk drawer that others can access).
- For Information about HIPAA Privacy/Security Rule Legislation go to: http://www.hhs.gov/hipaa/for-professionals/index.html

Dear Healthcare Worker,

Your confidentiality breach was not just about getting caught or getting in trouble – it's about how your choices left a patient/parents feeling betrayed by a trusted professional. Even though you did this without malicious intent, the fact of the matter is that you didn't just mention how cute our little one is … you also felt the need to bring out very personal and unique information about them –the diagnosis and treatment. Why was that necessary? It makes me feel like our child was put on display, objectified, and used to entertain or impress others.

Having the same diagnosis myself, I have experienced the heartbreak of others treating me in this same manner - as a novelty, something that you talk about because it's so strange or different from the norm. I know our child will unfortunately be subject to these experiences – but I never imagined it would happen at the hands of a health care professional.

My hope is that you will take this to heart and realize the impact that your breach has had on our entire family. I hope that you will use this experience to become a strong advocate for fiercely and strictly guarding the confidentiality of your future patients' private and personal health information … not because you will get in trouble if you don't, but because you realize the emotional impact that any betrayal of this nature has on the mental health and well-being of the patients who trusted you.

Sincerely,

Your Patient/Family

~NOTES~