Being a Good Steward of Patient Data

By Marti Arvin, Executive Advisor
CynergisTek, Inc.

Being a good steward of protected health information (PHI) means understanding the laws and policies, collecting only the information needed, and using it only for the purposes for which it was collected.

Sharable with Fundraisers UNDER HIPAA

- NAME
- ADDRESS & OTHER CONTACT INFORMATION
- AGE
- GENDER
- DATE OF BIRTH
- DEPARTMENT OF SERVICE
- TREATING PHYSICIAN
- OUTCOME INFORMATION
- INSURANCE STATUS

Best Practice

Some parts of the law need to be interpreted by the covered entity and a guiding policy implemented.

You Can Share PHI for Fundraising if the Covered Entity...

- Includes a provision in notice of privacy practice (NPP)
- Informs of the right to opt-out
- Includes opt-out information in all fundraising solicitations

PHI can be used internally, disclosed to an institutionally related foundation, or shared with a business associate if a Business Associate Agreement (BAA) is in place.

Is it Always Considered PHI?

Individually Identifiable Health Information (IIHI) is PHI if:

- ✓ It is held by the covered entity
- ✓ It is held by the covered component of a hybrid entity
- ✓ Shared with a business associate supporting the covered entity's fundraising efforts

It is Not PHI if:

- ✗ The information is in the possession of an institutionally related foundation
- ✗ The foundation receives IIHI from a donor and subsequently shares it with a vendor supporting fundraising efforts

Using the Data

You Have a Responsibility to...

- Ask for the minimum information to accomplish your intended goal.
- Work to achieve a balance between increasing funding for mission critical functions with the goal of protecting patient privacy.
- Follow your organization's established security and data governance policies.

Work with the Compliance Officer to...

- Discuss the data needed and for what purpose to determine compliance with organizational, state, and federal laws.
- Determine the information that can be legally shared, and also what the organization should share.
- Take a "big picture" approach to data requests to simplify compliance and processes.

Securing the Data

You Have a Responsibility to...

- Follow your organization's policies designed to limit risk to system security.
- Work as a liaison between your technology providers and the internal information security team.
- Be familiar with the fundraising system capabilities and the security controls of the locations where data is stored.

Work with the Compliance Officer to...

- Protect PHI through encryption, multi-factor authentication (if available), and follow acceptable use policies.
- Use automation to set very specific parameters around the data that is shared by the covered entity with the fundraising organization.
- Follow good data governance practices.

Dig deeper into HIPAA and fundraising, including the regulations, roles and compliance.

Learn more

blackbaud

DISCLAIMER: All the opinions in this article are the author's own and don't reflect the opinions of Blackbaud. Further, nothing in this article is intended to be legal advice—please consult your organization's own legal counsel.