Caring

Geisinger

HIPAA and Privacy Overview For Our Business Associates

Geisinger Privacy Office

Introduction

- At Geisinger, we take the privacy and confidentiality of our patients, members and employees very seriously

- If you receive protected health information (PHI) regarding Geisinger patients or members in the course of your contractual duties, unless an exception applies, you are required to sign and abide by the terms and conditions of a business associate agreement (BAA).

The following slides are intended for informational purposes, and highlight some of the requirements of HIPAA and the BAA. All Business Associates (BAs) are required to be familiar with the terms and conditions of the BAA and have appropriate controls in place to comply with HIPAA and other applicable state and federal privacy laws.

Business Associate Agreements

All Business Associates are required to have a valid up to date BAA signed and executed by all parties.

The contact information in the BAA should be up to date at all times. If the contact information in the BAA changes, please contact Geisinger so we can update the information.

If you hire a subcontractor and provide them with any PHI, you are required to ensure that they sign a BAA.

Training

All Business Associates are responsible for providing privacy training to ***all*** individuals who will be exposed to protected health information (PHI) regarding Geisinger patients or members.

Business Associates are required to keep records of the training for audit purposes.

Safeguards

All Business Associates are required to abide by the HIPAA Security Rule and have reasonable technological, physical, and administrative safeguards to protect PHI.

All Business Associates are expected to have appropriate privacy and security policies in place and to conduct periodic risk assessments.

Breaches

If a BAA or a subcontractor of a BAA, uses PHI inappropriately or discloses PHI to an unauthorized individual or entity, the event should be reported to Geisinger as soon as possible.

To report breaches[1], please refer to your BAA or contact Geisinger's System Privacy Office at 570-271-7360 or systemprivacyoffice@Geisinger.edu

[1]Geisinger does not expect to be notified of unsuccessful Security Incidents which are defined as pings, broadcasts attacks on firewalls, port scans, unsuccessful log-on attempts, denial of service attacks, and similar events that do not result in unauthorized access or use of Protected Health Information and which do not materially affect the integrity and availability of services provided to Covered Entity by Business Associate.

Permissible Uses of PHI

Business Associates will only use PHI as permitted by the business associate agreement. In particular, unless specifically allowed, business associates shall not:

- Use or further disclose Protected Health Information other than as expressly permitted or required by this BAA or as required by law
- Transmit or store PHI offshore, outside of the domestic United States
- De-Identify PHI for sale or use by other entities

Other Laws

In addition to HIPAA, Business Associates agree to abide by all applicable privacy and security laws which may include but are not limited to:

- Confidentiality of Alcohol and Drug Abuse Patient Records Regulation (42 CFR Part 2)
- Pennsylvania Breach of Personal Information Notification Act (73 PS 2301, et seq)
- Other applicable federal and state laws

NOTE: Please consult with your legal counsel to determine which laws are applicable to you.

References

To learn more about HIPAA and Business Associate obligations please visit:

https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html