



What is Protected Health Information?

PHI (Protected Health Information) is any information related to the health status, provision of healthcare, or payment for healthcare that can be linked to an identifiable (specific) individual and is collected by a Covered Entity (a health plan, provider or clearinghouse) or its Business Associate (a vendor that processes PHI on the Covered Entity's behalf).

PHI may also include data that falls into the category of SPI (Sensitive Personal Information), which is highly sensitive information that if lost or inadvertently disclosed could result in substantial harm or embarrassment to an individual. Examples of SPI vary across organizations but may include:

- SSN
- Date of Birth
- Biometric or Genetic Records
- Political or Religious views
- Race or Ethnicity
- Sexual Orientation
- Bank Account Numbers

Do individuals have a right to download their Protected Health Information from Castlight's secure platform?

Yes. Under HIPAA (Health Insurance Portability and Accountability Act), if a Covered Entity or Business Associate maintains a Designated Record Set (comprehensive healthcare records) pertaining to an individual, that individual has a right to access and transmit their PHI. And although Castlight does not maintain Designated Record Sets of data, we follow HIPAA guidance and permit users of our platform to access and download certain PHI.

Source: Department of Health and Human Services: [Individuals' Right under HIPAA to Access their Health Information 45 CFR § 164.524](#).

What are some of the risks associated with downloading Protected Health Information from Castlight's secure platform?

Some of the risks associated with downloading PHI into an unsecure environment include:

- Lack of encryption and lack of protection for PHI
- Unauthorized access to PHI by a third party
- Loss or theft of device storing the downloaded information
- Improper disposal of the device



What are some recommended safeguards prior to downloading Protected Health Information from Castlight's secure platform?

Castlight strongly recommends setting up the following safeguards on your device before downloading PHI:

- Ensure your mobile or desktop device is encrypted
- Enable password protection on all endpoints
- Transmit any downloaded data via a secure channel

Are there any additional considerations?

Under the HIPAA Privacy and Security Rules, while Castlight is responsible for ensuring reasonable safeguards in accommodating an individual's request to download their PHI, Castlight is not responsible for PHI downloaded into an unsecure environment by that if it notifies the individual of the risk involved. In such cases, Castlight provides a warning to the individual and confirms that the individual still wants to receive PHI in this manner.

Source: Depart of Health and Human Services: [Individuals' Right under HIPAA to Access their Health Information 45 CFR § 164.524](#).

Where can I go for more information on this topic?

For general inquiries regarding Castlight's Privacy practices, please refer to our [Policy Statement](#). For additional information and resources on this topic please refer to the [Department of Health and Human Resources Website](#) or email Castlight's Privacy Team at: Privacy@castlighthealth.com