Protected Health Information (PHI) Handling Guide

Learn what constitutes PHI and how to properly handle it on your website

What is PHI?

Protected Health Information (PHI) is any information about health status, provision of health care, or payment for health care that can be linked to a specific individual.

18 HIPAA Identifiers

PHI includes any of the following 18 identifiers when combined with health information:

- [ ] Names (full or last name and initial)
- [ ] Geographic subdivisions smaller than a state
- [ ] Dates (except year) related to an individual
- [ ] Telephone numbers
- [ ] Fax numbers
- [ ] Email addresses
- [ ] Social Security numbers
- [ ] Medical record numbers
- [ ] Health plan beneficiary numbers
- [ ] Account numbers
- [ ] Certificate/license numbers
- [ ] Vehicle identifiers and serial numbers
- [ ] Device identifiers and serial numbers
- [ ] Web URLs
- [ ] IP addresses
- [ ] Biometric identifiers (fingerprints, voiceprints)
- [ ] Full-face photos
- [ ] Any other unique identifying number or code

Common Website PHI Scenarios

Patient portals: Require secure authentication and encryption

Contact forms: Avoid collecting PHI unless absolutely necessary

Appointment scheduling: Use secure, HIPAA-compliant systems

Email communications: Never send PHI via unencrypted email

Analytics: Ensure no PHI is sent to third-party analytics tools

Best Practices for PHI on Websites

- [ ] Minimize PHI collection - only collect what is necessary
- [ ] Use secure forms with SSL/TLS encryption
- [ ] Implement strong authentication for patient portals
- [ ] Never display PHI in URLs or query strings
- [ ] Ensure third-party tools (chat, analytics) are HIPAA compliant
- [ ] Provide clear privacy notices
- [ ] Train staff on PHI handling procedures