HIPAA Compliance Datasheet

HIPAA Compliance SurveySparrow

Your business's privacy & security is our top priority. And, that's exactly why we treat the safe custodianship of your data as our core function. Collectively referred to as HIPAA, the Health Insurance Portability and Accountability Act of 1996 along with a series of supplemental regulations, sets national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge.

In terms of Experience Management Software, the solution & security architecture must comply with all the applicable standards & implementation specifications that protect the confidentiality of Protected Health Information (PHI) stored, handled or processed by the covered entities or business associates.

HIPAA security standards state that the covered entity must:

- Secure the integrity, confidentiality & availability of all electronic PHI
- Detect and safeguard against any foreseeable threats or risks to the security of the information
- Protect against any reasonably anticipated impermissible uses or disclosures of such information
- Certify compliance by their entire workforce

How SurveySparrow Enables HIPAA Compliance

We are committed to comply with all applicable data protection laws. We are a defined Business Associate and as part of our HIPAA compliance, SurveySparrow enforces and maintains the appropriate administrative, technical and physical safeguards for ensuring the confidentiality, security, integrity and privacy of the PHI. And in the capacity of a Business Associate throughout the duration of providing services to our healthcare customers, SurveySparrow platform enables HIPAA compliance to covered entities.

Signing the Business Associate Agreement with SurveySparrow is a mandatory requirement to enable HIPAA Account, please contact your account manager for more details.

Additionally, we have executed agreements with our subcontractors that create, receive, maintain, or transmit PHI on our behalf which contains the same restrictions, conditions, reasonable and appropriate safeguards that apply to SurveySparrow with respect to such PHI under HIPAA.

Please note that HIPAA enabled accounts cannot be reverted back into a regular account.

The following table demonstrates the HIPAA standards, and SurveySparrow's approach to comply with it.

Standard	How SurveySparrow supports HIPAA
Access Control	Multi-layered access control for owner, admin, and contributors. The admin has complete control of the account and the users, with features such as roles & access.
Encryption	All data is encrypted in transit, end to end, and at rest using industry-standard Advanced Encryption Standard (AES) encryption using 256-bit keys to protect data encryption. Log data is also encrypted to mitigate risk of ePHI stored in log files. Data encryption protects against passive and active attacks on confidentiality.
Unique User Identification	All users within the SurveySparrow environment are issued a unique username and password.
Automatic Logoff	SurveySparrow systems settings on all of its servers have session timeout features enabled.
Audit Controls	SurveySparrow has policies in place addressing audit trail requirements. Systems within its environment are logged to a centralized logging solution, which monitors system level events and contains a user ID, timestamp, event, origination, and type of event. These logs are constantly monitored for suspicious events and alerts are generated if any are found.

Integrity	SurveySparrow has a centralized access control system for authenticating and accessing internal systems where ePHI resides. Multilayer integration protection is designed to protect both data and service layers. Accounts on the internal database are restricted to a limited number of personnel with multi-factor authentication, and logging in place to track all transactions.
Person or Entity Authentication	SurveySparrow has a policy that describes the process of verifying a person's identity before unlocking their account, resetting their password, and/or providing access to ePHI.
Minimum Risk to Architecture	SurveySparrow leverages a redundant and distributed architecture to offer a high level of availability and redundancy.
Transmission Security	Data transmission is protected using HMACSHA-256 message authentication codes. Load balancers segment the traffic and send transmissions of the data to the application servers via an encrypted connection using HTTPS. All internal servers are accessed through a bastion host which is not accessible from the internet and requires an SSH connection.
Response and Reporting	SurveySparrow has anIncident Response Plan that sets the procedures for identifying, responding to, and escalating all suspected or confirmed security breaches. We also have an IRP team to effectively deal with possible security breaches, immediately.

Disaster Recovery Plan	SurveySparrow has a Disaster Recovery plan to help the efficient recovery of critical business data & systems in the unfortunate event of a disaster. The DR plan includes technical procedures to reinstate the infrastructure and data to allow critical business functions to continue the business operations after a disaster has occurred. To ensure the effectiveness, SurveySparrow performs annual testing of the DR plan without fail.
Business Associate Contracts	SurveySparrow has a policy and process in place for performing due diligence with any third party or vendor before engaging them.

HIPAA Security best practices

Action	HIPAA Security Tips
Exporting survey results	When downloading survey results, encrypt the downloaded files to secure them. And, to transfer them under an encrypted connection.
Sharing surveys with others	When sharing the survey, please make sure that you're sending it to the right recipients, and have been authorized to send the survey.
Managing the survey account	When adding teams, or users,please make sure that they've been authorized to access the survey. The collaborators will be able to view/share the survey results.

Collecting responses	We do not recommend the use of an Email Invitation as email survey invitations to recipients carry a unique survey link tied to a recipient's email address. If respondents are allowed to edit their responses, a recipient of an email invitation could complete all or part of a survey and forward their unique survey link to someone else. This would allow the second recipient to view the first recipient's responses, which may contain PHI. If you collect PHI in your survey, we recommend Link share.
Sharing survey results	Your survey results may contain PHI. Please ensure that you disclose results only to authorized recipients, and we also recommend enabling password protection.

HIPAA Certification

The agencies responsible to certify health technology – the Office of the National Coordinator for Health Information Technology and the National Institute of Standards and Technology – do "not assume the task of certifying software and off-the-shelf products" (p. 8352 of the Security Rule), nor accredit any other independent agencies to do HIPAA certifications.

It should also be noted that the HITECH Act only supports testing and certification of Electronic Health Records (EHR) programs and modules. As SurveySparrow is not an EHR software or module, our area of technology cannot be certified by these unregulated agencies.

SurveySparrow's HIPAA Attestation was performed by a third party that reviewed and affirmed that our environment & services has implemented the appropriate controls needed to secure PHI in accordance with the requirements of the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, Breach Notification Rule, and the applicable parts of the Privacy Rule. Additionally, the Attestation was conducted in compliance with the American Institute of Certified Public Accountants (AICPA) Statement on Standards for Attestation Engagements (SSAE) 18, AT-C sections 105 and 205.

Other Security Certification

ISO/IEC 27001

ISO/IEC 27001:2013, an internationally recognised standard for implementing Information Security Management System (ISMS) ensuring confidentiality, integrity & availability of information within the organisation