HIPAA Compliance Datasheet

HIPAA (Health Insurance Portability and Accountability Act) is a federal law enacted in the United States in 1996. HIPAA is a set of established rules that are designed to protect the privacy and security of individuals' health information.

The Privacy Rule standards address the use and disclosure of individuals' health information—called "protected health information".

The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.

The general requirements of HIPAA Security Standards state that covered entities must:

- Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
- Ensure the use of inclusive practices and meaningful participation of ALL children.
- Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the privacy regulations.
- Ensure compliance by its workforce.

How Swivl Reflectivity support HIPAA Compliance

Swivl provides Reflectivity web-based software that allows the collection of video artifacts and collaboration between teachers, instructional coaches, and admins that create opportunities for coaching, self-reflection, and collaboration for improving teaching practices and achieving the professional learning goals of the project.

The Reflectivity platform is designed to ensure that all confidential customer data that we collect remains secure and protected.

To meet the requirement of the HIPAA Security Rule, Swivl uses multiple layers and types of controls to secure our platform to ensure confidentiality, integrity, and availability of data. We have implemented generally accepted standards of technology and operational security in order to protect personal information from loss, misuse, alteration, or destruction.

Additionally, we have executed agreements with our subcontractors that receive, maintain, or transmit any Personal Information on our behalf which contains the same restrictions, conditions, reasonable and appropriate safeguards that apply to Reflectivity.

It is the customer’s responsibility to understand if electronic PHI is included in user-generated information and data. The customer is responsible for the security of the workstations and systems that are used to generate or view PHI within their information systems.

Implemented Safeguards

To facilitate our customers' compliance with HIPAA security regulations, we are providing detailed information about the security safeguards we have implemented into the Reflectivity service. The following table demonstrates how Reflectivity support HIPAA compliance safeguards with The HIPAA Security Rules, published in the Federal Register on February 20, 2003 which specifies a series of administrative, technical, and physical security procedures for covered entities to use to assure the confidentiality, integrity, and availability of e-PHI.

Administrative Safeguards

HIPAA Standard	Swivl Implementation
Security Management Process • Organizations must conduct risk analyses, implement measures to reduce risks and vulnerabilities, implement a workforce sanctions policy, and implement procedures to review system activity.	• Swivl implemented and documented the security management process, developed security policies and procedures that reflect it. These policies and procedures cover various aspects of information security, including administrative, physical, and technical safeguards. We conduct risk assessment on regular basis in accordance with NIST SP 800-30.
Workforce Security • Members of the workforce should have clearance before accessing systems containing ePHI and measures must be implemented to limit access to ePHI and terminate access when they change roles or end their employment.	• Swivl provides comprehensive training to all employees and contractors who have access to personal information. We implemented appropriate access controls to ensure that only authorized individuals have access to customer data. We establish procedures for revoking access privileges and promptly removing system access for employees who leave the organization or change roles and conduct it quarterly.
Information Access Management • This standard applies to hybrid and affiliated organizations to ensure ePHI is only accessed by members of "covered" organizations´ workforces and not by workforce members of parent, joint, or affiliated organizations.	• Access to all personal customer data is limited for employees and granted just for performing their job duties. Swivl has implemented RBAC. We regularly review and update access privileges. We implemented password complexity rules and MFA for staff. We have a continuous monitoring and logging system for tracking all audit logs and recording access inside the information system with alerting if any unusual or anomalous activities are identified.
Security Awareness and Training • Members of the workforce – even those with no access to ePHI – must participate in an ongoing security awareness training program. This standard also includes security reminders and password management.	• We perform security awareness training annually for all employees and for every new hired employee before granting access to our information system. We control completing Security Awareness Training for all staff.
Security Incident Procedures • Associates to adopt measures for reporting, responding to, and documenting the outcomes of security incidents (Note: Not limited to cybersecurity incidents).	• For incident management we developed and documented Incident Response Plan, where we described all processes for incident handling.

Contingency Plan

• Establish (and test) policies and procedures to respond to an emergency. The policies and procedures must include a data backup plan, a disaster recovery plan, and an emergency mode operating plan.	• We have documented an Information System Contingency plan and Contingency Planning Policy that contain detailed procedures for recovery. In addition, we have a number of sub-processes that ensure our business continuity. We also have documented Disaster Recovery Plan and test it quarterly.

Periodic Evaluations

• This standard requires Covered Entities and Business Associates to periodically review the policies, procedures, and measure implemented to comply with the Security Rule – including Business Associate Agreements.	• We review and update on a regular basis security-related documentation, including policies, procedures, and incident response plans, to ensure they are current and accurately reflect implemented security controls. We conduct regular vulnerability scans to identify vulnerabilities in the organization's systems and applications and implement necessary improvements.

Physical Safeguards

HIPAA Standard	Swivl Implementation
• The Physical Safeguards focus on physical access to ePHI irrespective of its location.	• We are a SaaS platform that is hosted on AWS. AWS is a reliable cloud provider that implements a set of physical safeguards and comply with all listed requirements. More details about physical safeguards implementation can be found by the link.

The HIPAA Technical Safeguards

HIPAA Standard	Swivl Implementation
Access Control	
• This standard not only relates to user identification and password management, but also includes implementation specifications relating to automatic logoff, encryption, and emergency access procedures.	• Swivl has implemented Role-Based Access Control for granting access to employees in accordance with their duties. We require strong passwords for all accounts accordingly implemented password complexity rules (min 10 char. with a mix of numbers, uppercase letters, lowercase letters, numbers, and special characters) Swivl requires MFA for all employees accounts at all related services. • Reflectivity encrypts all data in transit using TLS 1.2 and SSL certificates from a trusted authority. • All data is encrypted at rest through the AES-256 algorithm. Customers can select data center regions for data storage. Reflectivity logically separates data using built-in application logic controls. Our platform supports unique user identification. All users within the platform are assigned a unique User ID that is tied to the Enterprise ID.

Audit Controls

- A covered entity must implement hardware, software, and/or procedural mechanisms to record and examine access and other activity in information systems that contain or use e-PHI.

- Swivl has documented Audit security policy and procedure, that defines the specific events and activities that are logged and monitored within an information system.

Integrity Controls

- Electronic measures must be put in place to confirm that e-PHI has not been improperly altered or destroyed.

- Web and application access are protected by verified email address and password. Swivl implemented a process for detecting unauthorized changes to the information system and uses system for tracking that changes continuously to files, as well as identifying who made the change. Also we use encryption techniques to protect the integrity of data during transmission and storage. TLS 1.2 in transmission and AES-256 at storage.

Transmission Security

- A covered entity must implement technical security measures that guard against unauthorized access to e-PHI that is being transmitted over an electronic network.

- Reflectivity has implemented encryption mechanisms to secure the transmission of customer data. Reflectivity uses secure communication protocols, such as HTTPS and TLS 1.2, to transmit data securely over networks.

Policies and Procedures and Documentation

- A covered entity must adopt reasonable and appropriate policies and procedures to comply with the provisions of the Security Rule.

- Swivl has a set of implemented security policies, and procedures, incident response and contingency plans that establish comprehensive security safeguards to protect user personal data and PHI. We have a process of reviewing this documentation on a regular basis. Also, we conduct an independent auditor to check our policy compliance with the NIST standard accepted by HIPAA.

Swivl Reflectivity HIPAA Certification

There is no HIPAA certification for a cloud service platform, such as Reflectivity. In order to meet the HIPAA requirements applicable to our operating model, Reflectivity aligns our HIPAA risk management program with TX-RAMP and NIST 800-53, which are higher security standards that map to the HIPAA Security Rule. NIST supports this alignment and has issued SP 800-66 An Introductory Resource Guide for Implementing the HIPAA Security Rule, which documents how NIST 800-53 aligns to the HIPAA Security Rule.

Swivl is a reflective technology company. Our solutions help educators develop the four essential skills needed to navigate the rapidly changing world: adaptability, connecting with peers, becoming intrinsically motivated, and self-regulation. Founded in 2012, Swivl is headquartered in Menlo Park, CA with employees around the world.

Visit swivl.com | Follow @goswivl