Wickr
HIPAA & HITECH White Paper

Wickr® provides secure and ephemeral collaboration applications that help health care workers and organizations comply with the Health Insurance Portability and Accountability Act (HIPAA) safeguards to protect their information while in transit over communication networks and at rest on organizational devices.

Before we get into the details, this document assumes you have a basic understanding of HIPPA, HITECH, and what a covered entity is, and what e-PHI is. If you don't, please go to the HHS.gov site (https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html) first and then come back to this document.

By definition, Wickr is not a "covered entity" or a "business associate". Wickr provides secure and ephemeral collaboration applications to assist in adhering to your organization's compliance journey. It's important to realize that using Wickr does not mean you are now fully HIPPA compliant. Wickr's applications helps your organization comply with HIPPA rules when securely communicating or transmitting e-PHI.

First lets understand the HIPPA General Rules for compliance:

General Rules:

- The Security Rule requires covered entities (those that need to be HIPPA compliant) to maintain reasonable and appropriate safeguards to protect e-PHI in the categories of:
    1. administrative
    2. technical
    3. physical

Specifically, covered entities must:

4. Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit;
5. Identify and protect against reasonably anticipated threats to the security or integrity of the information;
6. Protect against reasonably anticipated, impermissible uses or disclosures; and
7. Ensure compliance by their workforce.[4]

The Security Rule defines “confidentiality” to mean that e-PHI is not available or disclosed to unauthorized persons. The Security Rule's confidentiality requirements support the Privacy Rule's prohibitions against improper uses and disclosures of PHI. The Security rule also promotes the two additional goals of maintaining the integrity and availability of e-PHI. Under the Security Rule, “integrity” means that e-PHI is not altered or destroyed in an unauthorized manner. “Availability” means that e-PHI is accessible and usable on demand by an authorized person.

Below are the three categories listed (Administrative, Physical, Technical) with the safeguards as outlined in HIPPA. In red is how Wickr can help with each safeguard or “Outside of Wickr” where the safeguard must be met by policy or other means.

Administrative Safeguards

- **Security Management Process**. As explained in the previous section, a covered entity must identify and analyze potential risks to e-PHI, and it must implement security measures that reduce risks and vulnerabilities to a reasonable and appropriate level. Having a data and communication policy that govern the use of Wickr when securely communicating or transmitting e-PHI.
- **Security Personnel.** A covered entity must designate a security official who is responsible for developing and implementing its security policies and procedures. Wickr can provide guidance to your security official on the proper use of Wickr; however, the policies and procedures squarely fall within the responsible organization.
- **Information Access Management.** Consistent with the Privacy Rule standard limiting uses and disclosures of PHI to the "minimum necessary," the Security Rule requires a covered entity to implement policies and procedures for authorizing access to e-PHI only when such access is appropriate based on the user or recipient's role (role-based access). Wickr allows organizations to control who has access to information and how long the information exists. Organization authorized personnel can implement secure Rooms/Conversations that follow the adhere to the organization’s policies and procedures; and, secure Wickr network setup can allow for this for communication and transmission use cases.
- **Workforce Training and Management.** A covered entity must provide for appropriate authorization and supervision of workforce members who work with e-PHI. A covered entity must train all workforce members regarding its security policies and procedures, and must have and apply appropriate sanctions against workforce members who violate its policies and procedures. Wickr can provide Wickr administrator & Wickr end-user training under your direction in conjunction with your policies.

- **Evaluation**. A covered entity must perform a periodic assessment of how well its security policies and procedures meet the requirements of the Security Rule. Responsibility of the organization, while providing feedback on proper use and guidance of Wickr.

Physical Safeguards

- **Facility Access and Control.** A covered entity must limit physical access to its facilities while ensuring that authorized access is allowed. At no time does Wickr or any of its employees have access to your data.
- **Workstation and Device Security.** A covered entity must implement policies and procedures to specify proper use of and access to workstations and electronic media. A covered entity also must have in place policies and procedures regarding the transfer, removal, disposal, and re-use of electronic media, to ensure appropriate protection of electronic protected health information (e-PHI). The Wickr application can be configured for secure authentication of use. Additionally, it will meet your transfer policy and its ephemerality (think short term purge) can help you meet your removal and disposal policy.

Technical Safeguards

- **Access Control.** A covered entity must implement technical policies and procedures that allow only authorized persons to access electronic protected health information (e-PHI). As a function of administration, you will only add authorized persons to your network to allow access. There is further control at the group level where participants must be explicitly invited to participate.
- **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. Outside of Wickr
- **Integrity Controls.** A covered entity must implement policies and procedures to ensure that e-PHI is not improperly altered or destroyed. Electronic measures must be put in place to confirm that e-PHI has not been improperly altered or destroyed. The Wickr encryption prevents unauthorized altering or destruction of the content – organizations and authorized organization personnel have complete control how long content exists.
- **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. The Wickr encryption prevents unauthorized access in transit and at rest.