Privacy and Security FAQ

What data does Securly collect?

The data collected is dependent on which service(s) your organization uses. However, Securly never collects, stores, sells, trades, or accesses any PII (Personally Identifiable Information), PHI (Personal Health Information), or Financial information.

Securly Content Filtering- School email address, public IP address (available to anyone on the Internet), visited websites, search terms, YouTube videos, and social media posts (if social media is allowed by the school).

Auditor- School email address, email subject and body. This data is only stored if the sender or recipient matches a current customer in our system and if words and/or phrases are flagged as grief, self-harm, or cyberbullying by our Sentiment Analysis Engine.

Parent Portal- Parent first name, Parent last name, Parent email, student first name, student last name, student email.

What privacy assurances do we have that Securly won't sell our data or be hacked?

Securly is committed to protecting the privacy and security of all customers and their end-users. We've implemented a multi-pronged approach to provide vault-like protection.

1. **Compliance**- Every process and procedure is created with compliance in mind. In addition to being iKeepsafe certified, we are committed to complying with the Family Education Rights and Privacy Act (“FERPA”) and the Children’s Online Privacy Protection Act (“COPPA”) in all applicable respects with regards to the collection, use, disclosure, and retention of the PII of minors.

2. **Localization**- All US customer data is transmitted and stored on servers located in the United States. Data is also broken up into two clusters: US-East and US-West. This helps to containerize data.

3. **Vulnerability Management**- Securly contracts a third-party firm to actively penetration test our infrastructure when we're least expecting it. This is to help mimic a real-world scenario.

Additionally, Securly has obtained Cybersecurity breach insurance.

Is Securly CIPA, FERPA, HIPAA certified?

Children's Internet Protection Act ("CIPA")
Currently, no vendor certification of CIPA exists. There is a CIPA checklist which is owned by each individual entity that is E-rate funded. Securly may very well be the only single solution that helps schools and libraries become fully CIPA compliant with web filtering and email scanning (Auditor).

According to FCC.gov "Schools and libraries subject to CIPA are required to adopt and implement an Internet safety policy addressing:

- Access by minors to inappropriate matter on the Internet;
- The safety and security of minors when using electronic mail, chat rooms and other forms of direct electronic communications;
- Unauthorized access, including so-called "hacking," and other unlawful activities by minors online;
- Unauthorized disclosure, use, and dissemination of personal information regarding minors; and
- Measures restricting minors' access to materials harmful to them."

Refer:
https://www.fcc.gov/consumers/guides/childrens-internet-protection-act

FERPA and COPPA

"We are committed to complying with the Family Education Rights and Privacy Act ("FERPA") and the Children's Online Privacy Protection Act ("COPPA") in all applicable respects with regards to the collection, use, disclosure, and retention of the Personally Identifiable Information of minors. However, please note that as a school, district, or educational institution, you may also possess certain legal obligations with respect to such Personally Identifiable Information. Please consult with your own legal counsel to ensure your compliance with applicable federal and state laws, as we do not take any responsibility for your failure to comply with the requirements of FERPA or COPPA."

HIPAA

HIPAA does not apply to web filtering. Securly does not create, receive, transmit, or maintain any PHI. In the event, Securly servers were used to proxy such information, Securly respects and obey all security measures taken by the end server/service. This means Securly will never downgrade a connection's security. The data will always be as safe as it were without use of Securly.

"1. Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit;

2. Identify and protect against reasonably anticipated threats to the security or integrity of the information;

3. Protect against reasonably anticipated, impermissible uses or disclosures; and

4. Ensure compliance with their workforce."

Refer:

https://www.securly.com/privacy

https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html