

# PathwAI

## **PHI Breach Notification Policy**

Version 1 - Approved by Abdullah Adeeb

# PHI Breach Notification Policy

PathwAI Labs is committed to safeguarding Personal health information (PHI) and we are committed to compliance with laws regulating the processing and protection of PHI. Thus it is important for all PathwAI Labs staff to understand their responsibilities in protecting and processing PHI as a part of our regular business operations.

If PHI is acquired, accessed, used, or disclosed in a manner not permitted under HIPAA or in a manner that compromises the security or privacy of the PHI, it may be considered a Breach. Specifically, a breach shall have the meaning given under 42 U.S.C. § 17921(1) and 45 C.F.R. § 164.402.

In the event of a breach or a suspected breach, please follow the steps outlined below:

## Reporting of Suspected Breach

Any PathwAI Labs staff member who discovers a potential breach of unsecured PHI shall report it to the company's Information Security Officer immediately.

## Investigation of Suspected Breach

1. The Information Security Officer shall review the circumstances of the suspected breach to determine if the incident was intentional or unintentional. Certain unintentional incidents described more fully below, do not constitute reportable breaches (although they may still constitute violations of the HIPAA Security Rule or Privacy Rule).
  1. If PHI was acquired, accessed, or used by a staff member of PathwAI Labs, but the acquisition, access, or use was made in good faith and within the scope of permitted activities of the staff member, and there is no further unpermitted use or disclosure, then this does not constitute a breach.
  2. If PHI was inadvertently disclosed by one staff member of PathwAI Labs to another staff member, and there is no further unpermitted use or disclosure, then this does not constitute a breach.
2. The Information Security Officer shall review the circumstances of the suspected breach to determine if the incident poses a significant risk of financial, reputational, or other harm to the customer. The risk assessment shall be documented. If the risk assessment results in a conclusion that the incident could cause a significant risk of harm, notification will be made as described in the Breach Notification section below.

## Breach Notification to Covered Entity

1. PathwAI Labs shall, following the discovery of any Breach of PHI, notify the appropriate Covered Entity in writing of such breach without unreasonable delay and in no case later than sixty (60) business days after discovery. The notice shall include the following information if known (or can be reasonably obtained) by PathwAI Labs:

1. Contact information for the individuals who were or who may have been impacted by the Breach (e.g., first and last name, mailing address, street address, phone number, email address);
2. A brief description of the circumstances of the Breach, including the date of the Breach and date of discovery (as defined in 42 U.S.C. § 17932(c));
3. A description of the types of unsecured PHI involved in the Breach (e.g., names, social security numbers, date of birth, addresses, account numbers of any type, disability codes, diagnostic and/or billing codes, and similar information);
4. A brief description of what PathwAI Labs has done or is doing to investigate the breach, mitigate harm to the individuals impacted by the Breach.

## Mitigation

PathwAI Labs shall mitigate, to the extent practicable, any harmful effect that is known to the company of a use or disclosure of PHI in violation of its business associate agreements.

## Non-Compliance

It is important to have appropriate penalties for any violations of our Breach notification policy. PathwAI Labs management will determine how serious a staff member's offense is and decide the appropriate penalty. Penalties may include a warning (oral/written) or suspension or termination for more serious offenses.

## Questions

If you have any questions regarding this policy, please reach out to your policy owner.

---

End of PHI Breach Notification Policy. For version history, please see the next page.

## Version History

Version	Log	Date
1 <b>Current</b>	Policy version approved by Abdullah Adeeb	02 Dec, 2025
1	New policy version created	02 Dec, 2025