M-Path and HIPAA compliance

What is HIPAA?

HIPAA is the Health Insurance Portability and Accountability Act. It imposes privacy and security mandates on health care providers and most of their IT vendors. The key components of HIPAA include ensuring that personally identifiable medical information remains private and secure. This law has made electronic medical records safer for patients but also comes with regulations for medical providers and their IT partners. In summary, any company or individual subject to HIPAA that deals with protected health information (PHI) must enact and enforce appropriate policies, procedures, and safeguards to protect data.

What is PHI?

PHI stands for Protected Health Information. PHI refers to any individually identifiable health information that is created, received, used, maintained, or transmitted by a covered entity or business associate in connection with an individual's health condition, treatment, or payment for the treatment. So, it encompasses details like medical records, diagnoses, treatments, and payment history. HIPAA regulations are primarily focused on safeguarding PHI to ensure patient privacy and security.

Is m-Path HIPAA compliant?

Yes, in so far as that m-Path under regular circumstances doesn't collect PHI-conform data. The PHI-standard excludes so-called "de-identificated data", which is data that has been rid of all 18 categories of what is deemed personally identifiable data:

1. Names
2. All geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP code, and their equivalent geocodes, except for the initial three digits of the ZIP code if, according to the current publicly available data from the Bureau of the Census:
   2.1. The geographic unit formed by combining all ZIP codes with the same three initial digits contains more than 20,000 people; and
   2.2. The initial three digits of a ZIP code for all such geographic units containing 20,000 or fewer people is changed to 000
3. All elements of dates (except year) for dates that are directly related to an individual, including birth date, admission date, discharge date, death date, and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older

4. Telephone numbers
5. Vehicle identifiers and serial numbers, including license plate numbers
6. Fax numbers
7. Device identifiers and serial numbers
8. Email addresses
9. Web Universal Resource Locators (URLs)
10. Social security numbers
11. Internet Protocol (IP) addresses
12. Medical record numbers
13. Biometric identifiers, including finger and voice prints
14. Health plan beneficiary numbers
15. Full-face photographs and any comparable images
16. Account numbers
17. Any other unique identifying number, characteristic, or code, except as permitted by paragraph (c) of this section [Paragraph (c) is presented below in the section "Re-identification"]; and
18. Certificate/license numbers

m-Path as a software platform does not collect any of the data above, so it deals exclusively in de-identified data (unless the research requires otherwise, see next section).

Do I have to do anything to remain HIPAA compliant?

m-Path allows researchers and practitioners complete freedom to collect data, so one can imagine that, even though m-Path itself doesn't collect PHI, a researcher or practitioner might structure their surveys in a way that does collect such data. As such, to remain in an agreement that is viable under HIPAA law, the covered entity also commits to a few measures to ensure compliance:

I. The covered entity does not use m-Path surveys to collect data that could be considered PHI (see the list above)
II. The covered entity informs participants or clients sufficiently to not provide any identifiable information in questionnaires or in m-Path itself (for instance, the m-Path nickname they provide).
III. In case the covered entity uses invitation codes, the covered entity ensures not to disclose the re-identification to any third party (nor m-Path itself), nor to use the invitation code as a means to identify the user in any other way besides on the m-Path platform itself.

Some examples of data-collection that fall outside of this commitment:

- Asking a participant to fill out their full name
- Adding a field to enter an e-mail address (to partake in a sweepstakes for instance)
- Asking for a birth day (birth year is fine)
- Having the participant record their own voice or photograph their own face
- Using a "Location" question module to get a participant's approximate location

- Using the m-Path participant nickname or invitation code as a key in some other platform (ie. Qualtrics, Google Forms…)

These measures may be codified in the m-Path license agreement, so please inform us if HIPAA compliance is a must for your organisation.