Model Policy on Data Privacy

This model policy is designed to provide examples of language that health departments (and other agencies) and facilities that offer healthcare can use and adopt to promote public health through the protection of private health information. Not all parts will be applicable to or within the jurisdiction of every aforementioned body. Technical requirements (e.g. encryption, data storage, hardware, etc) necessary to protect health data are beyond the scope of this policy. For the purposes of this model policy, health data is data (information) that is created, intentionally or not, in whatever form (analog or digital) when a person is engaged in seeking information regarding a health condition, seeking treatment for a health condition, or receiving treatment for a health condition, whether or not this is on behalf of themselves or another person.

MODEL POLICY

In order to improve public health, encourage the uninhibited use of medical services, and promote uncensored communication between health service providers (hereinafter "providers") and health services users (hereinafter "users"), it shall be the policy of [this agency/service provider] to ensure that unnecessary and potentially harmful data is not collected [and/or] that all health data which is gathered is only used for the provision of health services to users. In order to provide comprehensive protections for users' private health data, we hereby adopt the following:

I. Applicability
   A. This policy applies to any and all data related to health services provided to a user, or that is employed by a user to learn about and/or procure health services.
      1. This [agency/service provider]'s policy is applicable to any legal entity (eg. provider, sub-contractor, agent, etc) subject to the jurisdiction of said [agency/service provider] that may purposefully or inadvertently collect, process, share, or sell user's health data.
      2. This policy applies to any and all forms of communication that are utilized by a user in order to communicate with their health services provider or to learn more about the services they are seeking.

3. In any situation where a user is asked to provide or may purposefully provide health-related data, they must be explicitly notified as to what the entity collecting that information will use it for.
    a) Such notice shall not be considered explicit if it is not easily apparent and understandable; and
    b) Notice buried within the text of a "user agreement" is not sufficient.

II. Control and Consent

A. [agency/service provider] affirmatively states that any and all health data, including that created while seeking services, is private to the user and can only be:
    1. used in such a way as they give their voluntary, unambiguous, and informed consent; and
    2. disseminated with their voluntary, unambiguous, and informed consent.

B. A user has the right:
    1. To know what health data is collected
    2. To know any and all ways that their data may be used
    3. To know how long their health data will be retained
    4. To delete their health data from databases (including their own Health Record) unless such deletion is explicitly barred by a federal statute
    5. To opt out of the collection of their health data, which includes the ability to withdraw a previously given consent.
        a) It must be as easy for a user to withdraw their consent as it was to give consent in the first place.

C. All health data is deemed "sensitive" and protected by default. Deidentification of data and/or aggregation of data into anonymous datasets does not cancel or limit a user's absolute control of their health data.[1]

III. Release to Third Parties

[1] Policy authors acknowledge that health data gathered by providers can provide an invaluable tool for researchers to use to promote public health, identify gaps or biases in service provision, and to generally ascertain what works and what doesn't. However, due to the historic and ongoing erosion of trust of the medical system by the continually disenfranchised, primarily Black and brown people, this policy promotes both transparency as well as the meaningful ability to opt out of having one's health data used in such research, even within a large, anonymous data set. It is only through taking clear and unmistakable steps to rebuild trust that the damage can be repaired, and the massive benefit of such a seismic shift be reaped.

A. Any health data that is created by a user when trying to access a health service or subsequently when they receive treatment shall only be accessible by the user, those to whom they explicitly grant access, or those for whom it is necessary to have access to further a user's stated treatment goals.
    1. Any data that is collected by, or provided to, a public health entity for the purpose of improving public health generally cannot be used for any punitive measures of any kind, including but not limited to in any civil, administrative, or criminal proceeding against the user.
        a) Any health data created or collected under the jurisdiction of this [agency/service provider] requested by a third party shall not be released even if based on an in- or out-of-jurisdiction warrant, subpoena, civil investigative document, or court order if such a request or order is made to subject the user to civil, administrative or criminal liability in that jurisdiction UNLESS such a disclosure is ordered by a court of competent jurisdiction, subject to the below following:
            (1) This [agency/service provider] affirmatively states that it only considers valid a warrant, subpoena, civil investigative document, or court order if it is properly domesticated and served under the applicable law.
            (2) Regardless of its validity, this [agency/service provider] will take any and all legal action, including but not limited to filing in the proper court, to quash, reject, or limit compliance with any warrant, subpoena, civil investigative document, or court order if such a request or order is made to subject the user to civil, administrative or criminal liability.
            (3) If any health data is provided, it will be that which is the minimum required.
        b) Any health data created or collected under the jurisdiction of this [agency/service provider] shall not be released even if based on an in- or out-of-jurisdiction warrant, subpoena, civil investigative document, or court order if such a request or order is made to subject the provider to civil, administrative or criminal liability in that jurisdiction UNLESS so consented to by the user.

(1) If a user DOES NOT consent to the release of their health data:

(a) This [agency/service provider] affirmatively states that it only considers valid a warrant, subpoena, civil investigative document, or court order if it is properly domesticated and served under the applicable law.

(b) Regardless of its validity, this [agency/service provider] will take any and all legal action, including but not limited to fighting in the proper court, to quash, reject, or limit compliance with any warrant, subpoena, civil investigative document, or court order if such a request or order is made to subject the user to civil, administrative, or criminal liability.

(c) If any health data is provided, it will be that which is the minimum required.

2. This [agency/service provider] will immediately inform a user of any attempt by a third party to obtain their health data.
3. Any health data which is permitted to be transferred consistent with this policy must be the minimum necessary to carry out the specific purpose to which the user gave affirmative express consent.

B. Under no circumstances can any data gathered incidental to the access or provision of health services — including but not limited to location data, websites visited using wifi, or information garnered through the use of "cookies" — be sold or provided to any Third Party regardless of the stated use of such data by the Third Party.

IV. Harm

A. Disclosure or use of private health data in a way to which a user did not consent is admittedly in and of itself a "harm" in accordance with applicable tort law.

1. A user whose private health data has been so misused does not need to show damages — to one's finances, person, reputation, etc. — for a harm to be present. Such harm exists due to the fact that the user may be embarrassed, fear being discriminated against, or limit their own exercising of free speech in response to the misuse of data.