DRAFT: Principles for Health Community Rights on the Internet

Landscape

There is an urgent need to define a set of digital rights for health communities online. No rights yet exist for health communities online to protect the privacy and data that they collectively generate. Health Technology Platforms will need to embrace a new set of digital rights in order to sustain and preserve the value of the knowledge generated by online peer support communities.

Scope of Principles: Community Digital Rights

This set of digital rights is uniquely focused on health communities. Online health communities need to be able to trust that the platforms that they use to communicate with each other are not being used against them in any way.

What follows is a list of standards and requirements that health communities online should be able to expect from their technology platforms. This set of fundamental rights should be met by any technology platform interested in working with online [health?] communities, ensuring the protection of their digital and privacy rights.

Peer Support Community Rights

1: Right to proof of claims about privacy.

When working with online health communities, technology platforms must go further to ensure that claims about privacy, data-sharing, and data governance are backed with publicly verifiable evidence. It is not enough to say, "Trust us, we take your privacy seriously." Proof of claims includes ongoing audits to verify data-sharing practices, code reviews, or making code open source.

2: Right to a safe, clearly marked, and interoperable exit for online communities.

Online communities must have the ability to leave a service easily, as individuals or as a group, without losing access to the raw data or knowledge that has been gathered about their health while using the service.

3: Right to know the community's fair value.

Health communities must be able to clearly see all of the ways that a patient peer support platform is accessing and sharing data with third parties. For commercial platforms, health communities should also have the right to know the value of the data they have generated in any investment rounds or acquisitions.

4: Right to protect health vulnerabilities shared by communities or individuals.

Technology platforms must not use vulnerable information about health communities in a way that causes harm to the community as a whole or to individual members, or to allow third parties to do so. A platform must not engage in any sort of manipulation of

health communities' behavior without explicit disclosure and explicit community consent, or allow third parties to do so using the platform.

5: Right to disclosure of conflicts of interest.

Conflicts of interest exist when needs and interests of the online health community are not aligned with the business interests of the technology platform. Platforms must clearly disclose and handle conflicts of interest.

6: Honor the principles of Coordinated Disclosure of Privacy and Cybersecurity Threats (CDPCT) and embrace cybersecurity best practices.

The CDPCT standard outlines basic cybersecurity best practices and protocols for reporting security vulnerabilities for technology platforms dealing with health information generated by online communities.

7: Right to fair partnerships & good faith negotiations.

Communities have a right to expect fair business practices, and negotiation of fair partnerships when engaging with a tech platform. Good faith negotiations support the rights and interests of peer support communities to protect their privacy and autonomy. Fair partnerships may also include equal pay for equal work, and/or fair value that is generated on the tech platform through work done by online communities or online community moderators.

8: Right to data-sharing that follows established medical & research ethics.

This standard deals with how a platform conducts research by mining the data of an online health community. When research is conducted using the data of a community, all those involved in the research (e.g., platform, third parties) must have completed formal research/clinical ethics training. When health or safety studies are conducted knowingly in advance, even if only for internal or quality assurance purposes, the platform must show that they have gotten approval from an accredited ethics review board for the research. The ethics review board must specifically address the ethics of keeping internal research results from the study a secret, as well as other data and technology ethical questions.

9: Right to Community Representation from an information fiduciary.

A fiduciary is a person or business with an obligation, expertise, and capability to act in a trustworthy manner in the interest of another. Technology platforms who receive the “Light Collective Seal of Approval” will have proven their intention of fiduciary responsibility to patient communities who are sharing vulnerable health information through the platform.