Dr. Chatbot Notice of Privacy Practices

This Notice describes how the University of Rochester (“we”) uses a digital application for COVID-19 screening called Dr. Chatbot (also called “the Program”), to screen faculty, staff, students, contractors, volunteers, and visitors for possible infection with COVID-19, also known as novel coronavirus (the “coronavirus”). The Program’s primary purpose is to identify persons, before they enter the University’s property, who may be experiencing symptoms associated with the coronavirus.

This Notice also details the ways in which the University uses the information provided by persons who use Dr. Chatbot. It does not apply to the practices of companies or institutions that we do not own or control, or to individuals that we do not employ or manage.

Faculty, staff, students, contractor, volunteers, and visitor use of Dr. Chatbot may be required from time to time in order to reduce the risk to the University community from infection by COVID-19.

This Notice is subject to change from time to time with or without notice.

Acknowledgement of Terms:

By using the Program, you acknowledge that you have read and understood the information in this Notice.

Types of Information to Be Collected:

When you use the Program, you will have to log in with your University username and password (e.g., your Active Directory username), that identifies you as a faculty member, staff, student, contractor, volunteer, or visitor of the University. The Program will also collect information about how you feel and whether you have certain symptoms.

The Program may also automatically receive technical information relating to your usage of the Program such as identification of your operating system and device, Program features used, content viewed and downloaded, the dates and times of your interactions with the Program, and other similar information (“Technical Information”).

How Will This Information Be Used and Shared?

The University will use the information that you provide to operate a COVID-19 screening program. Specifically, we will use your answers to questions posed by the Program to determine whether you are experiencing symptoms that indicate you may be infected with the coronavirus. Your answers and other employee/student/contractor/volunteer/visitor information may be provided to the University Health Service (UHS) or URMC’s Employee Health Service, which may then contact you to provide information about seeking testing, follow-up health care, and/or some other steps you should take, up to and including quarantine practice.
The University will store the data as allowed by law and may use this information to understand and improve user experience with the Program.

With your specific consent, which you can give through the Program, we may also share your data in a de-identified, aggregated form with researchers, which may include healthcare organizations, academics, government agencies, public health authorities, as well as public or not-for-profit entities interested in health data. The University may also share de-identified, aggregate information with the general public through journal publications or postings in the effort to fight COVID-19. If you elect to provide this information, we may retain it for such time as necessary and appropriate to make the aforementioned uses.

We may use your contact information to communicate with you, including through email and/or SMS text messaging if you elect to provide such information. We may also provide contact information you choose to submit to the Program to public health authorities, if necessary to reduce a threat to your health and safety or that of others.

We may disclose information collected through the Program as required by law, when we believe disclosure is necessary to comply with a regulatory requirement, judicial proceeding, court order, or legal process served on us, or to protect the safety, rights, or property of the University or the public. We will not sell or share the information collected for advertising purposes.

HIPAA Inapplicable

Please note, since you are providing this information outside of a doctor’s office or hospital, your information and data is not subject to HIPAA (the Health Insurance Portability and Accountability Act). We will work to keep your information secure, as described below.

Is Personal Information and Technical Information about me secure?

We endeavor to protect the privacy of the Personal Information and Technical Information we hold in our records. Notwithstanding these efforts, we cannot guarantee complete security of the data. Unauthorized entry or use, hardware or software failure, and other factors, may compromise the security of your Personal Information and Technical Information at any time. In the event of such compromise, we will give you notice as required by law, and otherwise if feasible.

All information collected by the Program will be processed in the United States.

Effective Date and Changes to this Privacy Notice

This Privacy Notice is effective as of June 2, 2020. The University of Rochester may change this Privacy Notice from time to time. We encourage you to check this page for any new versions of this Privacy Notice. By continuing to access, browse, and/or use the Program, you agree to accept any posted revised terms.

This Notice is governed by and construed in accordance with the laws of the State of New York.
Questions or concerns?

If you have any questions or concerns regarding the topics addressed in this Privacy Notice, please send an email to: University of Rochester Office of Counsel or the University Health Lab.