Cyber4Healthcare Initiative Terms

June 3, 2020

Thank you for agreeing to be part of the Cyber4Healthcare initiative of the CyberPeace Institute.

These Terms are a binding agreement between the CyberPeace Institute and you. You have no right to join the Cyber4Healthcare initiative if you do not agree to these terms.

We also refer you to our **Privacy Policy**, which describes our privacy practices and is incorporated into these Terms.

NOTE: The Cyber4Healthcare initiative is not intended to facilitate or provide incident-response services. If you believe that you have suffered a compromise of your systems, you should inform the relevant law enforcement agencies and consider engaging a company in the business of responding to such compromises.

Introduction and The CyberPeace Institute Role

The Cyber4Healthcare initiative is intended to connect healthcare providers who require cybersecurity assistance (a "Requesting Entity") with entities that have the ability to provide such assistance (a "Provider"). The CyberPeace Institute will maintain information on Providers and Requesting Entities and will use reasonable efforts to match the needs of Requesting Entities with Providers. However, the CyberPeace Institute is not a part of any agreement between Providers and Requesting Entities, and you agree that the CyberPeace Institute will not be liable for any damages incurred by either a Requesting Entity or a Provider arising from or relating to their interactions, either with each other or with the CyberPeace Institute. The CyberPeace Institute does not guarantee that the assistance provided by a Provider will actually be useful to a Requesting Entity.

The CyberPeace Institute will perform a triage of incoming requests and may determine, in its sole discretion, that some requests are inappropriate for the Cyber4Healthcare initiative or that there are no Providers who are able to address the Requesting Entity's issue. As part of that triage, the CyberPeace Institute may determine that some requests are of lower priority than others and may delay in responding to requests it believes to be of lower priority. Of the requests that the CyberPeace Institute determines to be appropriate, the CyberPeace Institute does not promise that it will be able to connect every Requesting Entity with a Provider who is able to provide assistance.

The CyberPeace Institute will only provide your contact information to another member of the Cyber4Healthcare initiative with your permission. Until that permission has been granted, the CyberPeace Institute will keep the Requesting Entity and Provider anonymous.

Requesting Entity Responsibilities. Requesting Entity will:

1. provide accurate information regarding its cybersecurity assistance needs but will not provide more information than is necessary to evaluate its requests for assistance;

2. negotiate in good faith any agreements, including non-disclosure agreements, solely with Providers if its request for assistance is accepted by Institute. Requesting Entity is not required to work with any Provider and can refuse proposed Providers;

3. keep non-public information about Providers that it receives through the Cyber4Healthcare initiative confidential;

4. participate in debriefing and publication activities as described in the "Debriefing and Publications" Section below; and

5. maintain current and accurate information regarding its contact information with the Cyber4Healthcare initiative.

Provider Responsibilities. Provider will:

1. consider promptly and in good faith requests for assistance from Requesting Entities to help with one or more cybersecurity issues, which is intended to include in-kind or financial assistance. Provider is not required to accept any request for assistance;

2. negotiate in good faith any agreements, including non-disclosure agreements, with Requesting Entities if it accepts a request for assistance;

3. keep non-public information about Requesting Entities and their requests for assistance that it receives through the Cyber4Healthcare initiative confidential;

4. participate in debriefing and publication activities as described in the "Debriefing and Publications" Section below; and

5. maintain current and accurate information regarding its capabilities and its contact information with the Cyber4Healthcare initiative.

Confidentiality

When a Requesting Entity requests assistance through the Cyber4Healthcare initiative, the Requesting Entity may provide confidential or sensitive information, which might include information about security breaches, infection or cyberattack at the Requesting Entity. The CyberPeace Institute may pass this information on to Providers in order to help the Provider determine if it is able to assist the Requesting Entity. Otherwise, the CyberPeace Institute will take reasonable efforts to protect the information so disclosed. However, it is possible that, despite the CyberPeace Institute's efforts, information in its possession may still be compromised. The CyberPeace Institute will, upon request of a Requesting Entity, delete confidential or sensitive information previously provided by that entity.

Responsibilities of the actors seeking our assistance

We strive to protect the confidentiality and security of your data, and we ask that you likewise respect the privacy and security of our staff. When seeking assistance, you will be requested not to mention the name of, describe, or otherwise refer to the CyberPeace Institute staff for the purposes of being published any publicly available medium, including, but not limited to, newspaper, blog, social media post,

documentary. Any such sharing of our personal data may endanger our safety and security and therefore requires our written consent.

Debriefing and Publications

After a Provider has assisted a Requesting Entity, the three parties: CyberPeace Institute, Provider and Requesting Entity will engage in a "debriefing" discussion intended to provide information back to the CyberPeace Institute about issues discovered, trends, and potential future improvements to the Cyber4Healthcare initiative. Such information may include personal data and technical information about the case. The CyberPeace Institute may use information gained in the debriefing to deliver its products and services. With the permission of Requesting Entities and Providers, the CyberPeace Institute may publish testimonials and interviews describing the experience that Requesting Entities and Providers have had with the Cyber4Healthcare initiative. Providers and Requesting Entities agree to allow the CyberPeace Institute to use their names and logos in promotional activities relating to the Cyber4Healthcare initiative, subject to any trademark usage guidelines given to the Institute by the Provider or Requesting Entity.

Website Usage

The CyberPeace Institute operates a website at cyber4healthcare.cyberpeaceinstitute.org that will allow Requesting Entity to submit requests for assistance. The CyberPeace Institute does not guarantee that the website will function correctly or that it will be available at any particular time. The CyberPeace Institute may delete requests for assistance at any time, for any reason. By entering information about your organization into the website, you represent that you are authorized by your organization to do so, and that you have the authority to request cybersecurity assistance.