COMMUNITY BEHAVIORAL HEALTH CYBER SECURITY AWARENESS

Cyber incidents impacting our provider network have increased over the past several months. CBH is committed to the privacy and confidentiality of our members' information and providers' sensitive agency and fiscal data.

To help address the common vulnerabilities that we face, we are outlining the following guidelines should your organization experience a cyber-attack and/or your systems are compromised.

- Please notify your CBH Provider Representative **by telephone** as soon as possible of the incident. They will serve as your point of contact.
- Depending on the specifics of the situation, CBH will likely take the following actions:
  - Suspension of email communication between CBH and the provider/vendor
  - Suspension of direct deposit and use of manual checks picked up in person by an authorized agency representative.
  - CBH alert to the City of Philadelphia of the provider agency breach
  - CBH alert to our Claims vendor

These actions will likely remain in effect until receipt of a completed remediation plan.

CBH requests that all providers notify their assigned CBH Provider Representative if their agency has cyber liability insurance. We will update your provider file accordingly. If your agency does not have cyber liability insurance, we encourage you to explore your options.

Below are recommendations for action steps for immediate response to a cyber-attack. We urge providers to develop their own documented response plan that is accessible to staff if internal systems must be taken offline.

Immediate Response Protocol: Develop a predefined protocol for immediate response to a cyber-attack. This could include actions such as disconnecting affected systems from the network, notifying IT/security teams, and activating backup systems if available.

Patient Care Continuity: Ensuring patient care continues uninterrupted is paramount. Providers should consider manual processes or backup systems to use if electronic systems are compromised. This could involve paper-based records or alternative communication methods.

COMMUNITY BEHAVIORAL HEALTH CYBER SECURITY AWARENESS

Communication Plan: Clear communication is essential during a crisis. Please consider who needs to be informed about the situation, including external stakeholders such as regulatory authorities or law enforcement.

Security Measures: Plan for security measures to mitigate further damage and prevent similar attacks in the future. This could include strengthening passwords, updating software patches, or implementing additional security protocols.

Collaboration with IT/Security Teams: Coordinate closely with your agency IT and security teams to assess the extent of the breach, identify vulnerabilities, and implement remediation measures. This collaboration ensures a unified response to the cyber-attack.

Training and Awareness: Implement training sessions or awareness campaigns to educate staff about cybersecurity best practices. This could include recognizing phishing attempts, maintaining data safety, and reporting suspicious activities.

Regulatory Compliance: Healthcare providers must adhere to regulatory requirements regarding data protection and breach notifications. All actions taken during and after the cyber-attack align must with relevant regulations and guidelines.

Post-Incident Review: After the immediate crisis has passed, lead a post-incident review to evaluate the response, identify lessons learned, and make recommendations for improving future preparedness and resilience against cyber-attacks.

Please visit the **HPH Cyber Performance Goals** website for more details on steps to stay protected.

Please contact your Provider Representative or CBH IT at **cbh.tech-help@phila.gov** if you have any questions.