Cybersecurity Incident Reporting FAQs

The New York State Department of Health (NYSDOH) is providing the following FAQs to clarify the reporting of cybersecurity incidents.

1. **What is considered a reportable "cybersecurity incident" under the New York State Department of Health guideline?**

   Any event that affects patient care, or represents a serious threat to patient safety, including intrusions whose intent appears to be breach or theft of protected health records. Examples include, but are not limited to:

   a. Successful intrusions into a health care provider's information technology system (including those that are contracted out by the health care provider), network infrastructure, and/or medical equipment/devices.

   b. Ransomware attacks that disable all or part of information technology operations including administrative systems such as payroll, billing, or appointment scheduling.

   c. Cybersecurity incidents that have the potential to spread through established connections to other health care networks or government systems. Examples include file transfer systems or data reporting interfaces.

   If you are uncertain whether the event you are experiencing meets the examples shown above, please contact the NYSDOH Regional Office, at the number provided on the poster, to discuss.

2. **When does a provider need to report to the NYSDOH? Is the NYSDOH looking to get notification directly from individual employees or hear from IT/Security/Executive Management after validating a potential cybersecurity incident?**

   Provider staff should follow their established internal policies and procedures related to alerting their central IT/information security staff or IT vendor, of potential cybersecurity incidents. The incident should be validated before reporting to the NYSDOH Regional Office.

   Once it is determined that a cybersecurity incident is validated as credible and fits the definition of a cybersecurity incident as described above, facility-designated staff should report the incident to the applicable NYSDOH Regional Office.

3. **How to Report to New York State Department of Health?**

   Within 24 hours of receiving confirmation that a credible cybersecurity incident has occurred, ***all providers*** should:

   a. Follow the Cybersecurity Incident Reporting Protocol to call the NYSDOH Regional Office that covers your geographic location and report any cybersecurity incidents that meet the above definition

   b. The NYSDOH Regional Office will then provide instructions to the provider regarding any follow-up activities.