NEW YORK STATE OF OPPORTUNITY. Department of Health

**ANDREW M. CUOMO**
Governor

**HOWARD A. ZUCKER, M.D., J.D.**
Commissioner

**SALLY DRESLIN, M.S., R.N.**
Executive Deputy Commissioner

October 18, 2019
Revised OHIM DAL 19-01

Dear Administrator / Technology Officer:

The New York State Department of Health (NYSDOH) has implemented a new notification protocol that providers should follow to inform the NYSDOH when they have experienced a cybersecurity incident at their facility or agency. The attached poster provides contact information for each NYSDOH Regional Office. Providers should use this list to contact their respective NYSDOH Regional Office immediately at the onset of a cybersecurity incident. The Regional Office will then provide instructions to the provider regarding any follow-up activities.

We recognize that providers must contact various other agencies in this type of event, such as local law enforcement. The NYSDOH, in collaboration with partner agencies, has been able to provide significant assistance to providers in recent cybersecurity incidents. Our timely awareness of this type of incident enhances our ability to help mitigate the impact and protect the integrity of our healthcare delivery system and the public's health. Therefore, this protocol should be immediately implemented by all providers of the following types:

- Hospitals, nursing homes, and Diagnostic and Treatment Centers
- Adult care facilities
- Home Health Agencies, Hospices, Licensed Home Care Services Agencies (LHCSA)

These reporting instructions and the attached poster should be shared with your staff designated to report incidents for your facility or agency.

Thank you for your attention to this important activity. Please submit any questions you may have by email to: ohim@health.ny.gov

Sincerely,

Mahesh Nattanmai
Chief Health Information Officer
Office of Health Information Management

Attachment: Cybersecurity_ReportingGuide_poster.pdf
Cybersecurity Incident Notification FAQs Final.pdf

# 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.

# You're the Key to Reporting a Cybersecurity Incident!

**An incident is considered a reportable "cybersecurity incident" under the New York State Department of Health guideline, if it 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.

## Business Hours

8:30 am to 4:45 pm weekdays and non-holidays, unless noted

### Capital District — (518) 402-1036

Albany, Clinton, Columbia, Delaware, Essex, Franklin, Fulton Greene, Hamilton, Montgomery, Otsego, Rensselaer, Saratoga, Schenectady, Schoharie, Warren and Washington

### Central New York — (315) 477-8400

Broome, Cayuga, Chenango, Cortland, Herkimer, Jefferson, Lewis, Madison, Oneida, Onondaga, Oswego, St. Lawrence, Tioga and Tompkins

### Metropolitan Area — (212) 417-5550

9:00 am to 5:00 pm

Bronx, Kings, New York, Queens and Richmond

### Central Islip — (631) 851-8050

9:00 am to 5:00 pm

Nassau and Suffolk

### New Rochelle — (914) 654-7005

9:00 am to 5:00 pm

Dutchess, Orange, Putnam, Rockland, Sullivan, Ulster and Westchester

### Western Area — (716) 847-4505

Allegany, Cattaraugus, Chautauqua, Chemung, Erie, Genesee, Livingston, Monroe, Niagara, Orleans, Ontario, Schuyler, Seneca, Steuben, Wayne, Wyoming and Yates

## After Hours Emergencies

4:45 pm to 8:30 am weekdays. Available 24 hours a day on weekends and holidays

### NYSDOH Duty Officer — (866) 881-2809

Select option #1 for reporting an emergency.

## CALL 911 if there is immediate threat to public health or safety.

**In all cases, the cybersecurity incident should be reported to law enforcement.**

NEW YORK STATE | Department of Health