DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services
Centers for Clinical Standards & Quality
Information Systems Group
7500 Security Boulevard
Baltimore, Maryland 21244-1850

QualityNet Incident Response Procedures

Version 8.4

1 December
2022

Prepared by:
Ventech Solutions

TABLE OF CONTENTS

List of Figures

I. QUALITYNET INCIDENT RESPONSE PROCEDURES (IRP) REVIEW LOG

This Review Log is maintained to record reviews of the QualityNet IRP that have taken place over a three-year period. The review log should be completed by entering the data for each column in the appropriate row.

Date	Reviewer	Organization	Reason for Review or Update
5/21/2018	Tamara Hagerty	Ventech Solutions	Updated document to include SNow and contact information.
8/30/2018	Tamara Hagerty	Ventech Solutions	Review and update
4/2/2019	Tamara Hagerty	Ventech Solutions	Standardized terminology, aligned phases to RMH Chapter 8: Incident Response handbook.
9/23/2019	Brandon Tennessee	CMS	Approved by CMS
9/01/2020	Tamara Hagerty	Ventech Solutions	Updated Section III: Removed Paragraph 3 added bullet point Updated Section Updated URL Links Replaced QNet & QualityNet verbiage to QualityNet
10/07/2020	Ian Sheldon	CMS	Reviewed/lightly edited by Ian Sheldon, IS3, CMS
10/27/2020	Tamara Hagerty	Ventech Solutions	Reworded Section III first paragraph Reworded Section IV seventh paragraph
1/16/2021	Tamara Hagerty	Ventech Solutions	Reformatted review log table per CMS CCSQ ISSO guidance
12/1/2022	Rebecca Appah	Ventech Solutions	NIST and ARS Guidelines updated to most recent versions

II. INTRODUCTION

Compliance with the *QualityNet Incident Response Procedures* is mandatory. These procedures have been created as part of the Health Care Quality Improvement System (QualityNet) Security Program to act as guidance to the Centers for Medicare & Medicaid Services (CMS)/Center for Clinical Standards & Quality (CCSQ)/Information System Group (ISG) Management and CCSQ Business Owners in developing an incident response program in the event of computer-security incidents and/or adverse events involving the QualityNet General Support System (GSS) and its

major applications.

These procedures establish uniform guidelines for protecting and controlling information technology resources relating to QualityNet activities. The document ensures appropriate procedures will be put in place to minimize the risks and consequences of system intrusion, breach of information, and/or other adverse events.

PURPOSE & SCOPE

This document describes the methodology implemented by CCSQ to heighten the awareness of QualityNet system users to prepare for, respond to, and recover from incidents. For more detailed information on Incident Handling, see CMS Information Systems Security and Privacy Policy (IS2P2) V3.0, June 2022; Computer Security Incident Handling Guide, NIST Special Publication 800-61 Rev2 of August 2012; CMS Acceptable Risk Safeguards (ARS)) V5.0, June 2022 and CMS Risk Management Handbook (RMH) Chapter 8, V2.1, March 2021

These procedures are applicable to all QualityNet users, contractors, and others who process, store, transmit, or have access to CMS sensitive data, personally identifiable information (PII), electronic protected health information (ePHI), protected health information (PHI), and infrastructure computing resources that provide support within the QualityNet system infrastructure.

GOALS

The goals of the *QualityNet Incident Response Procedures* include:

- **Quick recovery**. The establishment of best practices for developing and implementing an incident response capability in accordance with organization policy, procedures, and standards to recover from security incidents quickly and efficiently.
- **Impact minimization.** Implementation of an incident response program to minimize loss or theft of information and reduce the effects of a disruption of critical computing services when incidents occur.
- **Systematic response.** Development of procedures to ensure timely, effective, and consistent response to incidents, as well as appropriate evidence collection and preservation.
- **System protection.** Establishment of ability to detect and respond effectively to a computer security incident to protect the confidentiality, integrity, and availability of Department of Health and Human Services (HHS) and its Operating Division (OPDIV) systems and data.

DEFINITIONS

This section provides definitions and explanations for terms used throughout this document.

1) Security Incident

1) The successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in any information system processing data on behalf of CMS. It also means the loss of electronic and hardcopy data through theft, device misplacement, and misrouting of mail; all of which may have the potential to put CMS data at risk of an intrusion, data breach or other adverse event.
2) An occurrence that jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits.
3) A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

2) Breach

Per CMS RMH V2, a breach is an incident that poses a reasonable risk of harm to the applicable individuals. For the purposes of Office of Management and Budget (OMB) OMB M-07-16 (for PII incidents) and Health Information Technology for Economic and Clinical Health (HITECH) Act (for PHI incidents) reporting requirements, a privacy incident does not rise to the level of a breach until it has been determined that the use or disclosure of the protected information compromises the security or privacy of the protected individual(s) and poses a reasonable risk of harm to the applicable individuals. For any CMS privacy incident, the determination of whether it may rise to the level of a breach is made (exclusively) by the CMS Breach Analysis Team (BAT), which determines whether the privacy incident poses a significant risk of financial, reputational, or other harm to the individual(s).

3) PII

1) PII is any information about an individual including, but not limited to education, financial transactions, medical history, and criminal or employment history; and information which can be used to distinguish or trace an individual's identity, such as the name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information, which is linked or linkable to an individual.
2) Information which can be used to distinguish or trace an individual's identity, such as the name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

4) PHI

PHI is individually identifiable health information that is transmitted by, or maintained in, electronic or any other form.

III. ROLES AND RESPONSIBILITIES

This section describes individual roles and responsibilities in support of the QualityNet incident response procedures.

QUALITYNET END-USER

- Immediately report all suspected security incidents to the locally designated Security Point of Contact (SPOC) and the user's supervisor. If no contact can be made with the SPOC, report the incident to the QualityNet Service Desk (SD).
- Work with the QualityNet SD, QualityNet SPOC, QualityNet Security Operations Center (SOC), and local Information Technology (IT) support staff to gather information and complete incident response activities.

QUALITYNET SPOC

- Contact the QualityNet SD (1-866-288-8912) to report any suspected security incident or by logging into ServiceNow and creating a Security Incident (SECINC) ticket.
- Serve as the ADO/Contractor functional system's point of contact for security incidents, as well as assist with the triage, response, and recovery phases.
- Prepare facility-level plans and procedures to address system security incidents in accordance with this document and security system standard operating procedures.
- Submit an Incident Report form to the QualityNet SOC within one hour of the incident, complete with all known information.
- Respond to all inquiries within one business day of the request or upon timelines as requested by the QualityNet SOC and/or the CMS QualityNet Information System Security Officers (ISSOs).
- Capture and securely store all evidence and/or artifacts relating to the incident. ***Do not destroy any evidence until the investigation is complete and explicit permission has been given by the QualityNet SOC and/or the CMS QualityNet ISSOs.***
- File any appropriate police report with local law enforcement.
- Provide technical support and advice for incident handling, impact assessment, and technical system management, including actions to be taken if circumstances are not covered by standard operating procedures.
- Report incident status and resolution information to management in accordance with this document and the standard operating procedures.
- Assist in information gathering, forensics, and reporting activities.
- Provide ad-hoc and periodic reports on security incidents and handling of advisories.

QUALITYNET SD

- Act as the first point of contact for system security incidents and records information provided by the QualityNet users, SPOCs, and local IT support.
- Document security incidents via ServiceNow SECINC tickets and assign them to the QualityNet SOC.

QUALITYNET SOC

- Submit Incident Report form for PHI/PII incidents to the CMS SD within one hour of the incident, complete with all known information.
- Follow proper internally documented procedures for reviewing and forwarding of applicable incidents to the CMS QualityNet ISSO; this includes coordination via the Incident Response Slack channel.
- Notify CMS SOC if PHI/PII event or at CMS QualityNet ISSO discretion.
- Engage SPOCs, support staff, and others to assist in responding, analyzing, containing, eradicating, and recovering from the incident.
- Follow-up with the SPOC, support staff, and/or end-user to obtain additional information where applicable.
- Serve as the custodian of all incident-related documentation.
- Respond to all inquiries within one business day of the request, or upon timelines as requested by the CMS QualityNet ISSOs.
- Capture and securely store all evidence and/or artifacts relating to the incident.
- Report incident status and resolution information to management in accordance with this document and other standard operating procedures.
- Provide ad-hoc and periodic reports on security incidents and handling of advisories.
- Assist in information gathering and reporting activities.
- Resolve and close ServiceNow tickets per CMS QualityNet ISSO guidance and procedures.

CMS QUALITYNET ISSOs

- Serve as an escalation point.
- Manage all incidents and report applicable incidents to the CMS and HHS privacy offices. Notify CMS QualityNet CISO and/or Federal authorities, *if required.*
- Serve as final authority on all incident resolutions, follow-on actions, and appropriate disciplinary methods, where applicable.

IV. REQUIRED ACCESS

Access to various environments and assets plays a key role when reporting and investigating a security incident. Unless written permission is given for a specific circumstance, all SPOCs are required to have the following accounts:

- QualityNet account
- HARP account
- ServiceNow account

ELECTRONIC COMMUNICATIONS

Electronic communications used throughout all phases of a security incident must be sent or received via QualityNet accounts. No third-party or commercial e-mail addresses are permitted. Internal e-mail can also be used to send encrypted attachments containing sensitive data such as Incident Report forms and any other artifacts pertinent to an incident. If e-mail is used, strict precautions must be exercised to include:

- Encrypted attachments pertaining to a security incident are only to be sent to members of the QualityNet SOC from an organization's designated SPOC unless otherwise directed by the CMS QualityNet ISSOs.
- Passwords must be sent in a separate medium such as a text message to a mobile phone or can be provided verbally over the phone. You cannot send the password in a separate e-mail message.

The Incident Report form should be encrypted and sent to the QualityNet SOC at SOC@hcqis.org, via Password Protected zip file attached to an e-mail or attached directly to the SECINC in ServiceNow.

Reference the QualityNet Rules of Behavior for additional guidance. Failure to take these precautionary actions will result in a security incident.

SERVICENOW

Access to ServiceNow is required for SPOCs to review the status of any open or closed security incidents for their sites. ServiceNow access is required for each SPOC for the QualityNet SOC to maintain an accurate list of each site's local SPOCs. Also, any user can now submit an Incident Response within ServiceNow. Current SPOC lists are maintained within ServiceNow and utilized by the QualityNet SOC and the CMS QualityNet ISSOs during investigations of security incidents or to seek other security-related information.

WHO CAN REPORT A SECURITY INCIDENT?

- Security Point of Contact (SPOCs)
- Anyone within the organization with access to ServiceNow
    - This may include any user that falls under QualityNet

SUBMITTING A SECURITY INCIDENT

- Submit a Security Incident in ServiceNow
- Email an Incident Response (IR) Form and send to the SOC at Soc@hcqis.org
- Report the Incident to the QualityNet SD (1-866-288-8912 and a Security Incident ticket will be created for the issue.
- Call the SOC on 571-1998-1999 and report the incident

Refer to Appendix G Steps for creating a ticket in Service Now

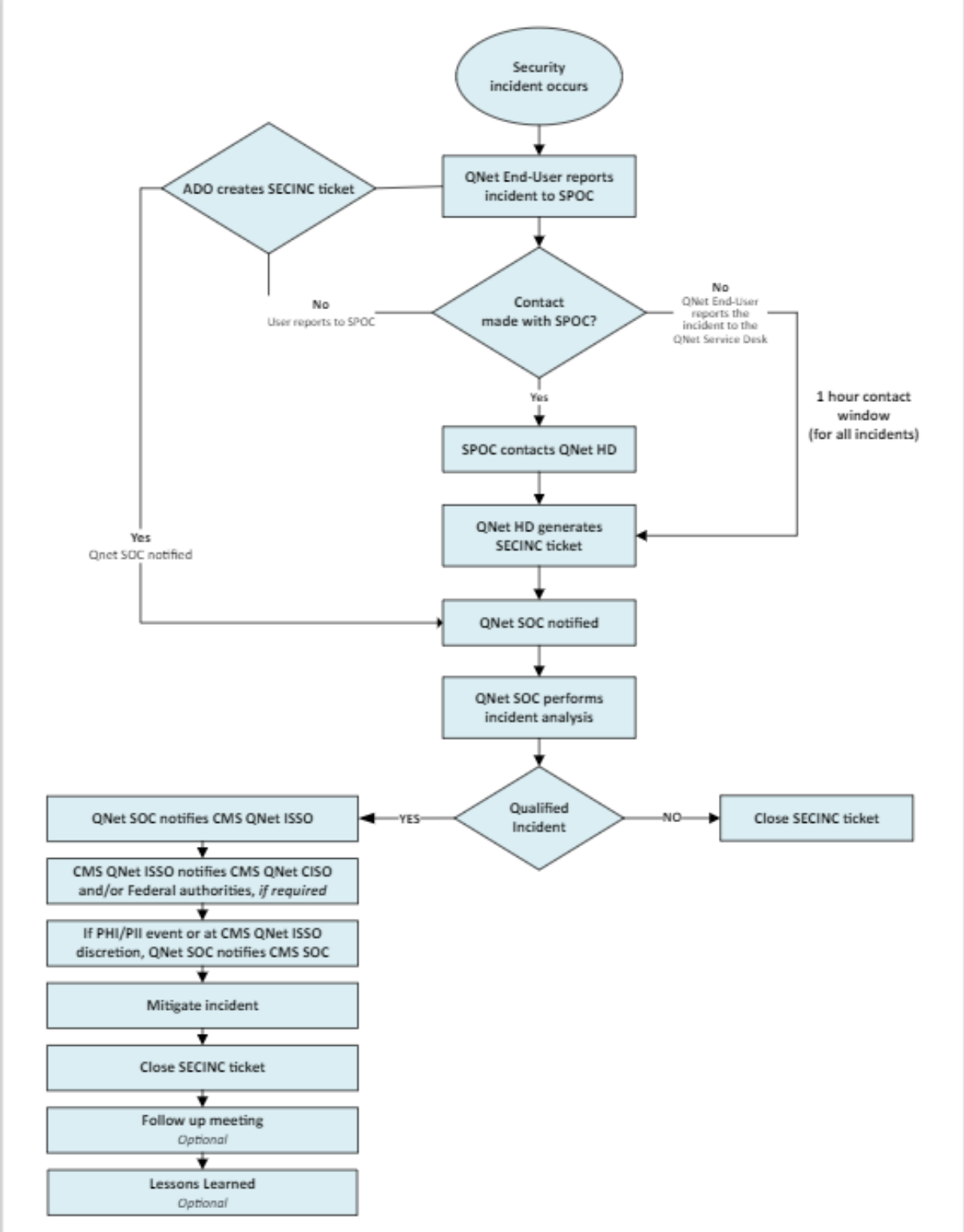
V. INCIDENT RESPONSE STEPS

The process of identifying an incident, opening a ServiceNow SECINC ticket, submitting the required documentation, and all follow-on efforts should be handled in accordance with the following steps.

- Identify that a security incident has occurred.
- Within one hour of identifying the security incident:
  a) As either the party identifying the event, or as the affected party, escalate the security incident to the local organization's SPOC. If you are the SPOC, proceed directly to contacting the QualityNet SD.
  b) Contact the QualityNet SD to have a security incident opened within ServiceNow.
- The SPOC will provide the QualityNet SOC with the completed Incident Report form via encrypted email or the ServiceNow SECINC ticket.
- The QualityNet SOC will gather the ServiceNow SECINC ticket number, the Incident Report form, as well as any other documentation for review.
- Following CMS policies and procedures, the QualityNet SOC will work with the CMS QualityNet ISSOs to investigate and document the security incident.
- The QualityNet SOC will reach out and work with the local organization and SPOCs as to the actions that should be performed to mitigate the incident.
- The SPOC is responsible for providing all additional information and forms within one business day, or upon timelines as requested by the QualityNet SOC and/or the CMS QualityNet ISSOs.
- Upon completion of the investigation, the QualityNet SOC will close out all ServiceNow SECINCs and notify the local organization of any applicable follow-on actions.

Figure 1 outlines the IR process flow.

Figure 1: IR Process Flow



VI. SECURITY INCIDENT INFORMATION AND GUIDELINES

Security incidents are classified according to impact on operations, system criticality, and the sensitivity of compromised data. After an incident is verified, incident response phases take place in order to restore operations and mitigate system vulnerabilities. Actions taken during the incident response phases vary according to type of incident. This section describes general guidelines for incident response phases for each incident security category.

The CMS RMH defines four phases of the incident response lifecycle as:

1) Preparation
2) Detection and analysis
3) Containment, eradication, and recovery
4) Post-incident activity

Understanding each phase facilitates responding more methodically and efficiently, and helps key staff understand the process of responding, so they can deal with unexpected aspects of incidents.

PREPARATION PHASE

The preparation phase of a security incident involves QualityNet personnel becoming familiar with applicable policies or procedures regarding how to respond to any potential security incident; as well as maintaining a state of preparedness by monitoring security tools. Being prepared to respond *before* an incident occurs is one of the most critical facets of incident handling. Advanced preparation avoids disorganized and confused response to incidents, as well as limits the potential for damage by ensuring that communication and response plans are known to all.
To facilitate that the proper preparations have been made to respond to information security and privacy incidents, CMS developed a checklist of activities to consider. The link to the checklist is contained in Appendix A, also located in the CMS Information Security and Privacy Library.

DETECTION AND ANALYSIS PHASE

Alerts may arise from a variety of sources including the United States Computer Emergency Readiness Team (US-CERT), user reports, monitoring of firewalls, network- and/or host-based detection systems, wireless intrusion detection systems, anti-virus software, threats received via email, and media reports about new threats.

The Detection and Analysis stage involves:

- Preparing for Common Attack Vectors
- Recognizing the signs of an incident
- Reporting and analyzing the incident
- Documenting the incident and updating in the Incident Response Reporting Template form and notifying the appropriate individuals. See Appendix A of this document for the Incident Response Reporting Template, also located in the CMS Information Security and Privacy Library
- Establishing a communication method and notifying the appropriate CMS personnel. Refer to Figure 1 in Section IV: Incident Response Steps.

When a staff member notices a suspicious anomaly in data, a system, the network, or an event, the QualityNet identification process should begin.

Preparing for common attack vectors

The attack vectors listed below are not intended to provide definitive classification for incidents; but rather, to simply list common methods of attack, which can be used as a basis for detection:

- **External/Removable Media**: An attack executed from removable media or a peripheral device, for example, malicious code spreading onto a system from an infected universal serial bus (USB) flash drive. **Attrition:** An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services (e.g., a Distributed Denial of Service (DDoS) intended to impair or deny access to a service or application; or a brute force attack against an authentication mechanism, such as passwords, CAPTCHAS, or digital signatures).
- **Web:** An attack executed from a website or web-based application; for example, a cross-site scripting attack used to steal credentials or a redirect to a site that exploits a browser vulnerability and installs malware.
- **Email:** An attack executed via an email message or attachment; for example, exploit code disguised as an attached document or a link to a malicious website in the body of an email message.
- **Impersonation:** An attack involving replacement of something benign with something malicious; for example: spoofing, man in the middle attacks, rogue wireless access points, and structured query language (SQL) injection attacks all involve impersonation.
- **Improper Usage:** Any incident resulting from violation of an organization's acceptable usage policies by an authorized user, excluding the above categories; for example, a user installs file sharing software, leading to the loss of sensitive data; or a user performs illegal activities on a system.

Recognizing the signs of an incident

The individual or team(s) involved examines all information available to determine whether or not a security incident has occurred. If an incident has occurred, the nature of the incident is determined, the initial priority level is assigned, and the documentation of all actions begins. All valid incidents will be assigned one of the categories described in Appendix C.

Typical signs of computer security incidents include any of the following:

- A system alarm or similar indication from an intrusion detection tool or other monitoring tool
- Suspicious entries in system or network accounting (e.g., a UNIX user obtains root access without going through the normal privilege escalation sequence)
- Accounting discrepancies (e.g., someone notices an 18-minute gap in the accounting log in which no entries appear)
- Unsuccessful log on attempts
- Unexplained new user accounts
- Unexplained new files or unfamiliar file names
- Unexplained modifications to file lengths and/or dates
- Inappropriate handling and transmission of PHI/PII data

- Unexplained attempts to write to system files or changes in system files
- Unexplained modification or deletion of data
- Denial/disruption of service or inability of one or more users to log in to an account
- System crashes
- Poor system performance
- Operation of a program or sniffer device to capture network traffic
- Unusual time of usage (incidents occurring outside of normal working hours)
- An indicated last time of usage of a user account that does not correspond to the actual last time of usage for that user
- Unusual usage patterns (e.g., programs are being compiled in the account of a user who does not know how to program)

Although no single sign conclusively shows that a computer security incident is taking place, the reporting of one or more of these signs shall prompt the QualityNet SOC to investigate events in a more thorough manner.

Reporting and analyzing an incident

When a potential incident has been identified, the next step is to report the incident so appropriate staff can be engaged and perform a more thorough analysis. Report the incident using the incident response steps in section IV.

Documenting the incident and notifying the appropriate individuals (Appendix A)
Information about the incident, such as dates, times and events that occurred, need to be documented in the Incident Response form and reported to the appropriate individuals. The Incident Response form can also be submitted as a ServiceNow SECINC ticket assigned to the HIDS Security SOC assignment group.

Establishing communication method and notifying the appropriate CMS personnel
Refer to Figure 1 – IR Process communication lines.

CONTAINMENT, ERADICATION AND RECOVERY PHASE

CONTAINMENT

The immediate objective for the containment, eradication and recovery phase is to limit the scope and magnitude of an incident as quickly as possible, and to gain evidence for identifying and/or potentially prosecuting the perpetrator. The first critical decision to be made during the containment and eradication stage is determining what to do with critical PHI/PII sensitive information and/or computing/network services.

A decision to determine the operational status of the compromised system (i.e., server, workstation, etc.) or information process itself shall be made to either:

1. Shut down the system entirely
2. Disconnect the system from the network

If there is a compromise of the information process, the following must occur:

1. Users must be re-trained.
2. Policies and procedures must be examined and perhaps re-written to correct the procedure.
3. The affected system shall be backed up to new unused media as soon as there are indications that a security incident has occurred. Making a full back up immediately captures evidence that may be destroyed before having a chance to study it.
4. Passwords must be changed immediately on all affected or compromised systems, as well as all systems that regularly interact with the compromised systems.

Identifying the evidence

To protect the evidence, the SPOC shall ensure all artifacts pertinent to the incident are clearly identified and labeled with appropriate dates, numbers (i.e., corresponding ServiceNow ticket numbers, artifact numbers, etc.), and sensitivity labels. Disks shall be sealed with original, unaltered, complete logs, or the entire log copied to an alternate location and secured appropriately. When turning over evidence to the QualityNet SOC, the SPOCs should ensure every item is signed for and detailed, factoring in the chain of command.

Protecting the evidence

The chain of custody for all evidence shall be preserved. Documentation shall be provided that indicates the sequence of individuals who have handled the evidence, the sequence of locations where the evidence has been stored, and the dates and times of the transfers. There shall be no lapses in time or date as the integrity of this information must be checked and provable in the anticipation that it may be challenged.

The QualityNet SOC and/or the CMS Security Operations Center (SOC) will require a full backup of the system in which suspicious events have been observed as soon as a computer security-related incident has been declared. Since perpetrators of computer crimes are becoming increasingly proficient in quickly destroying evidence of their illegal activity, be aware that, unless evidence is immediately captured by making a full backup, this evidence may be destroyed before it can be examined. This backup shall provide a basis for comparison later to determine if any additional unauthorized activity has occurred.

ERADICATION

The QualityNet SOC shall move quickly to eliminate components of the incident (e.g. delete malware, disable breached accounts, block malicious IP addresses) with minimal impact to the environment.

RECOVERY

The goal is to restore a system to its normal mission status or establish more effective user training. In the case of relatively simple incidents, recovery only requires assurance that the incident did not adversely affect the QualityNet network infrastructure or information resources. In the case of complex incidents, such as malicious code planted by insiders or the loss of PHI/PII data, recovery may require a complete restoration operation from backup tapes to pre-infection state.

The integrity of the backup shall be determined by attempting to read its data. Once the system has been restored from backup, the operation shall be verified as successful, and that the system is back to its normal operating condition. The local organization shall assist the QualityNet SOC, where applicable, to ensure the system is run through its normal tasks for monitoring.

POST-INCIDENT ACTIVITY PHASE

Following up on an incident after the containment, eradication and recovery period helps to improve incident handling procedures. This information is the basis for post-incident activity, which shall be documented and reviewed periodically. Answers to the following questions shall be considered to determine how well the QualityNet staff responded to the incident:

- Was there sufficient preparation for the incident?
- Did detection occur promptly? If not, why not?
- Could additional tools or processes have helped the detection and eradication process?
- Was the incident sufficiently contained?
- Was communication adequate? How could it have been improved?
- What practical difficulties were encountered?

During the incident response phases, the CMS Incident Report Form (Appendix A) shall be completed to aid in incident handling, decision-making, and reporting processes. The form shall be used to capture relevant information and attached to the SECINC ticket. Release of information during incident handling phases shall be exclusively on a need-to-know basis.

VII. REPORTING REQUIREMENTS

QualityNet users need to report incidents to the SOC (ServiceNow or via the PHI/PII process) as depicted in the Figure 1 – IR Process communication lines**.** Incidents should be reported to the QualityNet Service Desk within one hour (1-866) 288-8912 (internal and external) or email qnetsupport@cms.hhs.gov.

APPENDIX A – REFERENCES

CMS Incident Report Form
https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/RMH-Chapter-08-Incident-Response-Appendix-K-Incident-Report-Template

CMS Incident Preparation Checklist
https://www.cms.gov/research-statistics-data-and-systemscms-information-technologyinformationsecurityinformation/rmh-chapter-08-incident-response-incident-preparation-checklist

Federal Information Security Management Act (FISMA)
https://csrc.nist.gov/topics/laws-and-regulations/laws/fisma

RMH Chapter 08 Incident Response
https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/RMH-Chapter-08-Incident-Response

Health Insurance Portability and Accountability Act of 1996 (HIPAA)
https://aspe.hhs.gov/report/health-insurance-portability-and-accountability-act-1996

NIST Special Publication 800-61 Revision 2, Computer Security Incident Handling Guide
https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final

NIST Special Publication 800-66 Revision1, An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule
http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf

NIST Special Publication 800-122 Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)
https://www.nist.gov/publications/guide-protecting-confidentiality-personally-identifiable-information-pii

Office of Management and Budget (OMB) Circular A-130 Revised
https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf

QualityNet Rules of Behavior (ROB)
https://qnetconfluence.cms.gov/display/QNS/QualityNet+Security

QualityNet System Security and Privacy Policy (SSP)
https://qnetconfluence.cms.gov/display/QNS/QualityNet+Security?preview=/122686694/242194259/HCQIS%20Security%20and%20Privacy%20Policy%20Framework%20V1.0.pdf#QualityNetSecurity-Incident_Response

APPENDIX B – ACRONYMS

BAT	Breach Analysis Team
CCSQ	Center for Clinical Standards & Quality
CMS	Centers for Medicare & Medicaid Services
GSS	General Support System
ePHI	Electronic protected health information
HCQIS	Health Care Quality Improvement System
HHS	Health and Human Services
IP	Internet protocol
IS2P2	CMS Information Systems Security and Privacy Policy
ISG	Information System Group
ISSO	CMS QualityNet Information System Security Officers
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
OPDIV	Operating Division
PHI	Protected health information
PII	Personally identifiable information
RMH	Risk Management Handbook
SD	Service Desk
SECINC	ServiceNow security incident ticket
SOC	Security Operations Center
SPOC	Security Point of Contact
US-CERT	United States Computer Emergency Readiness Team

APPENDIX C – INCIDENT CATEGORIES

Category	Name	Description	Reporting Timeframe
PII	Personal Identifiable Information	Possible or confirmed compromise of any information about an individual maintained by an agency, partner, or contractor – for example, a Health Insurance Claim Number (HICN) or Social Security Number (SSN).	Within one hour of discovery/detection.
CAT 0	Exercise/Network Defense Testing	Used during state, Federal, national, international exercises, and approved activity testing of internal/external network defenses or responses.	Not applicable; this category is for each agency's internal use during exercises.
CAT 1	Unauthorized Access	A person gains logical or physical access without permission to a network, system, application, data, or other resource.	Within one hour of discovery/detection.
CAT 2	Denial of Service	An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources.	Within one hour of discovery/detection if the successful attack is still ongoing and the agency is unable to successfully mitigate activity.
CAT 3	Malicious Code	A virus, worm, Trojan Horse, or other code-based malicious entity that affects a host.	Daily. Note: Within one hour of discovery/detection if widespread across agency.
CAT 4	Improper Usage	A person violates acceptable computing use policies.	Weekly.
CAT 5	Scans/Probes	This category includes any activity that seeks to access or identify a federal agency computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service.	Monthly. Note: If system is classified, report within one hour of discovery.
CAT 6	Investigations	*Unconfirmed* Incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.	Not applicable; this category is for each agency's use to categorize a potential Incident that is currently being investigated.
CAT 7	Other	An attack does not fit into any other vector	Daily. Note: Within one hour of discovery/detection if widespread across agency.
CAT 8	Lost/Stolen Asset	The loss or theft of a computing device or media used by the organization	Daily. Note: Within one hour of discovery/detection.

APPENDIX D – EXTERNAL RESOURCES

The following list of incident response organizations may provide information related to an ongoing incident:

- United States Computer Emergency Readiness Team (US-CERT) – http://www.us- cert.gov
- CERT Coordination Center – https://www.sei.cmu.edu/about/divisions/cert/index.cfm
- Common Vulnerabilities and Exposures – http://cve.mitre.org
- Forum of Incident Response and Security Teams – http://www.first.org
- SANS Top 20
  - https://www.sans.org/critical-security-controls/
  - https://www.cisecurity.org/controls/
- United States Department of Homeland Security – https://www.dhs.gov/
- United States Department of Defense CERT – https://www.us-cert.gov/
- CMS QualityNet ISSOs – CMS-ISSO-Security@HCQIS.ORG
- QualityNet SOC – SOC@hcqis.org
- QualityNet Service Desk – qnetsupport@cms.hhs.gov

Note: hyperlinks are external and are subject to change at any time

APPENDIX E – EXTERNAL INCIDENT REPORTING PROCEDURES

PURPOSE

The purpose is to simplify and streamline the reporting of external PII/PHI incidents.

DEFINITIONS

External Incident – An external incident is one in which non-QualityNet users are responsible for physically or electronically sending PHI/PII to the QualityNet network or facilities. Examples include a clinician emailing unencrypted medical records to a QualityNet user and PHI/PII being included in a ServiceNow (SNOW) ticket (some non-QualityNet users have access to SNOW).

Internal Incident – An internal incident is one in which a QualityNet user is responsible for mishandling PHI/PII data. Examples include sending an unencrypted email containing medical records to a non-QualityNet user, storing PHI/PII on unapproved media, and sending an email to a non-QualityNet user containing internal network addresses in an unencrypted attachment.

PROCESS

- The SPOCs will record each incident as a separate row item in the spreadsheet
  - The SPOCs are responsible for submitting the spreadsheet, via a Service Now security incident (SECINC) ticket, within three days of an incident occurring. If a spreadsheet is not received the SOC will take the position that no incidents have occurred.
    - SPOC assigns SECINC to HIDS Security-SOC

  - SPOC attaches the spreadsheet to the ticket

- The SOC will review each incident to confirm the event was external
  - If all reported incidents are external, the SOC will close the SNOW ticket opened by the SPOC
  - If any reported incidents are internal, the SOC will create a SNOW security incident ticket for each misreported incident and assign to the SPOC for follow-up. The SOC will then close the SNOW ticket originally opened by the SPOC.
- The SOC will include the following in the weekly SOC report:
  - Total number of reported external incidents
  - External incidents reported by area/company/contractor

APPENDIX F – EXTERNAL INCIDENT REPORT TEMPLATE

Company			
SPOC			
Date of Incident	**Violator - Organization's Name**	**Violator - Individual's Name**	**Description of Incident**

APPENDIX G – CREATING A SECURITY INCIDENT IN SERVICENOW

The link below depicts the process of creating a Security Incident Ticket in ServiceNow.

- https://cmsqualitysupport.servicenowservices.com/nav_to.do?uri=/kb_view.do?sysparm_article=KB0023097