Weill Cornell Medicine

11.05

Security and Privacy Incident Response Plan

Responsible Executive: Chief Information Officer, WCM
Original Issued: October 1, 2007
Last Updated: November 12, 2020

Revision History:

Date	Author	Revision
November 8, 2018	Brian J. Tschinkel	Modified membership roles and breach notification requirements
November 12, 2020	Brian J. Tschinkel	Modified membership roles

Policy Statement

All members of Weill Cornell Medicine are responsible for protecting the confidentiality, integrity, and availability of data created, received, stored, transmitted, or otherwise used by the college, irrespective of the medium on which the data resides and regardless of format (e.g., electronic, paper, fax, CD, or other physical form).

In the event the confidentiality, integrity, or availability of data is compromised, and a suspected incident has occurred, the incident should be reported immediately to the Information Technologies & Services Department (ITS) or the Privacy Office. Reporting incidents quickly—regardless of certainty or magnitude—is critical to ensure the appropriate teams can respond and contain the incident as soon as possible.

Reason for Policy

Privacy and/or information technology (IT) security incidents can occur at any time and of varying magnitude. Identifying and resolving incidents in an organized systematic way is a vital component of our overarching compliance programs. This policy provides a framework for identifying, assessing, reacting to, communicating about, and documenting an incident and corresponding remediation plans.

Entities Affected by this Policy

The Weill Cornell Medical College and Graduate School of Medical Sciences

Who Should Read this Policy

All members of the Weill Cornell Medical College community.

Web Address of this Policy

https://its.weill.cornell.edu/policies/1105-security-incident-response

Contacts

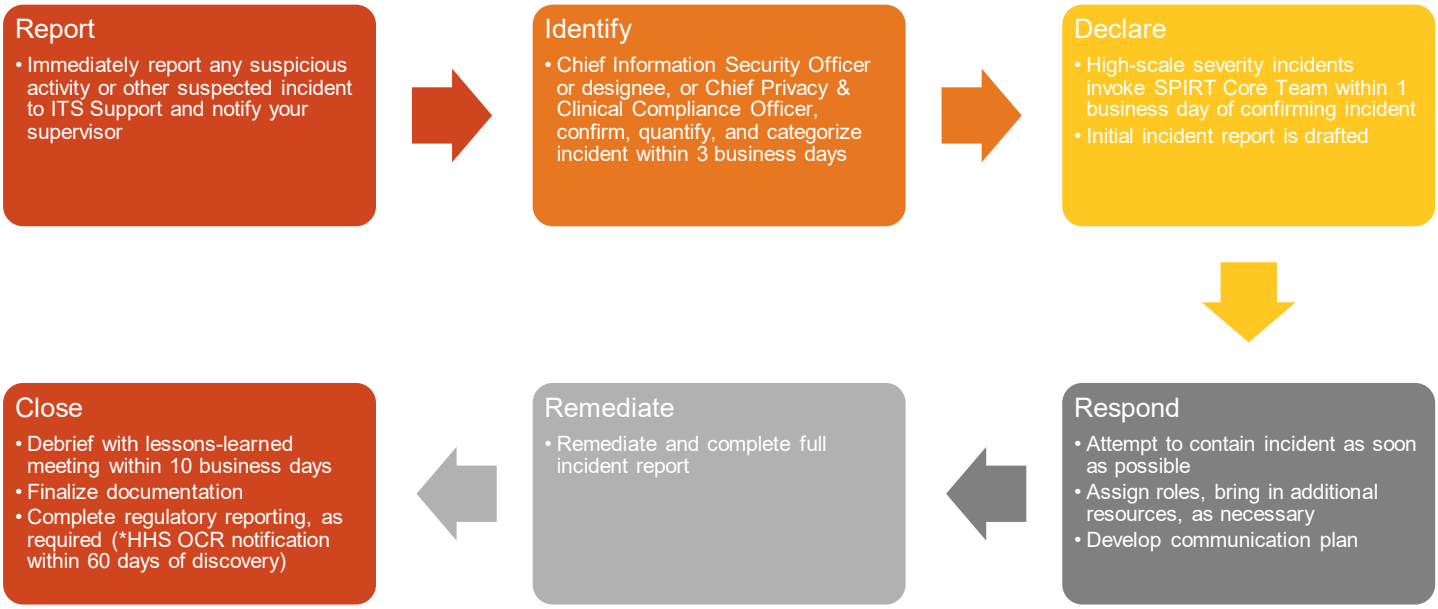
Direct any questions about this policy, 11.05 – Security and Privacy Incident Response Plan, to Brian J. Tschinkel, Chief Information Security Officer, using one of the methods below:

- Office: (646) 962-2768
- Email: brt2008@med.cornell.edu

Contents

1. Principles

Security and privacy incidents must be (1) reported, (2) identified, (3) declared, (4) responded to, (5) remediated, and (6) resolved with adequate record-keeping. Detailed requirements for each of these steps are below.



2. Reporting an Incident

If you know or suspect any unusual or suspicious behavior that does not match your expectation of good security or privacy management, immediately report the incident to your supervisor and ITS Support right away. Even if you are not certain or cannot confirm the incident, it's imperative that the incident is reported quickly so the right personnel can investigate as soon as possible.

To report an incident, notify your supervisor and contact ITS Support:

ITS Support
T (212) 746-4878
support@med.cornell.edu

If you wish to notify a compliance office directly or to report the incident anonymously, the following contacts can be used:

WCM Privacy Office
T (646) 962-6930
privacy@med.cornell.edu

WCM ITS Security
T (646) 962-3010
its-security@med.cornell.edu

Cornell Hotline (Anonymous)
T (866) 293-3077
http://hotline.cornell.edu

Filing or reporting an incident can be done without fear or concern of retaliation.

There are many different types of incidents that can be reported to ITS. Examples of incidents include, but are not limited to, the following:

- Patient information misdirected or disclosed via mail, fax, verbal means
- Medical record documents are misplaced, stolen, lost
- Medical record documents are exposed (e.g., files left open on computer), improperly disposed of (e.g., not shredded) or stored (e.g., not locked or protected)
- User accesses system or application with credentials other than his/her own
- Unauthorized access to a system, application, or document
- A device (e.g., laptop, smartphone, desktop, tablet, removable storage, smart watches, cameras, voice recorders, etc.) containing WCM data is lost, stolen, or otherwise unaccounted for
- A rogue device is connected to the network which impacts or prevents others from working
- System or individual is infected with malware or phishing (e.g., virus, ransomware)
- Potential data loss due to a malware infection

3. Identifying an Incident

Each reported incident must be investigated. Confirmed incidents will be categorized as follows:

A. Unauthorized or suspicious activity on WCM network, including systems or applications
B. WCM data is lost, stolen, misdirected to, or otherwise shared with an unauthorized party
C. A system on WCM network is unknown
D. A system on WCM network is infected with malware or otherwise compromised, targeted, or profiled
E. Other suspected compromise of data confidentiality, integrity, or availability

3.01 Identifying Affected Data

As quickly as possible, reasonable effort must be made to identify the type of data affected by the incident upon discovery and/or declaration. Various regulatory reporting and/or notification requirements, including deadlines, must be adhered to in accordance with applicable state, federal, or regulatory agencies. Such requirements include, but are not limited to, New York State Information Security Breach and Notification Act (ISBANA), Department of Health and Human Services Office of Civil Rights (HHS OCR), Office of Management and Budget Memorandum 07-16 (OMB M-07-16), and the Payment Card Industry Data Security Standard (PCI DSS), including any payment processors for Weill Cornell Medicine. This also includes the evaluation of the state of residence for affected individuals and any applicable reporting authorities.

By means of example, in accordance with OMB M-07-16, when “1) an individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resource; or 2) there is a suspected or confirmed breach of personally identifiable information regardless of the manner in which it might have occurred,” reporting to US-CERT is required within one hour of discovery/detection.

4. Declaring an Incident

Under the authority of the Chief Information Officer, the Chief Information Security Officer (or the designee), or Chief Privacy & Clinical Compliance Officer can declare a privacy or IT security incident. It is the responsibility of these individuals to evaluate the reported concern using the tools and risk assessment guides expeditiously to determine its authenticity and severity. Severity judgments will be based on ongoing persistent threats, the volume of data involved, and the potential for reputational and/or financial harm to the institution, or any affected individuals.

Low-scale severity incidents will be handled by the ITS Security & Identity Management team or the Privacy Office. For more severe incidents, the Chief Information Security Officer or Chief Privacy & Clinical Compliance Officer will convene into a meeting the core members of the Security & Privacy Incident Response Team (SPIRT) and begin drafting the initial incident report. The initial details of the incident will be discussed with the SPIRT core team at this time.

The primary purpose of SPIRT is to determine and guide the college's response to an information security or privacy incident, up to and including the need to satisfy existing data breach notification statutes or processes as well as an institutional decision to notify individuals of a breach of their personally identifiable or protected health information.

The SPIRT core team members include:

1. Assistant Vice Provost, Chief Information Officer
2. Chief Information Security Officer
3. Chief Privacy & Clinical Compliance Officer
4. Deputy University Counsel
5. Assistant Vice Provost, Communications & Marketing

As warranted by the type and scale of the incident, any of the SPIRT virtual team members may be convened by a core team member based on the type and scope of incident. Virtual team members provide assistance, advisement, and expertise from their representative areas. The SPIRT virtual team members include:

1. Director, Risk Management & Insurance
2. Assistant Dean, Clinical Research Compliance
3. Research Integrity Officer
4. Senior Associate Dean for Faculty
5. Senior Director, Human Resources Services
6. Department Administrator II, Graduate School
7. Associate Director, Medical Education Administration
8. Chief Medical Officer
9. Chief Medical Information Officer
10. Controller
11. Internal Audit Director
12. Chief Information Security Officer, Cornell University
13. University Auditor, Cornell University
14. Director, ITS (Weill Cornell Medicine-Qatar)
15. SVP, Chief Information Security Officer (NewYork-Presbyterian Hospital)
16. Chief Information Security Officer (Columbia University Irving Medical Center)
17. Chief Privacy Officer (NewYork-Presbyterian Hospital)
18. Chief Privacy Officer (Columbia University Irving Medical Center)
19. External Breach Response Resources

Other individuals not on the SPIRT core or virtual teams may be convened by a core team member based on the incident. Such individuals may include, but are not limited to, department administrators or subject matter experts.

5. Coordinating a Response to an Incident

5.01 Containing the Incident

Once an incident has been reported and declared, the incident must be contained to prevent further harm. By means of example, the following containment steps should be taken:

- For IT security-related incidents, such as an infected system on the WCM network, any network cables should be disconnected immediately, and the system should remain powered on to allow for further investigation.

- For incidents involving protected health information in paper form, immediate efforts should be made to retrieve any copies or gain assurances that all records are accounted for.

Effective containment stops damage from being done and allows assessment of the scope of the incident and the initiation of remediation activities.

5.02 Assigning Roles

Upon declaring the incident, the SPIRT core team members will convene the appropriate virtual team members—including any additional resources necessary, such as storage facilities, out-of-band communication channels, or additional staff—and assign roles pertaining to the incident assessment and response:

1. One incident commander
2. One incident coordinator
3. One IT forensics investigator
4. One data analysis investigator
5. One communications coordinator

The **incident commander** is responsible coordinating all stages of the incident response process, and specifically, acts as the leader of the investigation. In addition, the incident commander has the following duties:

- Ensures the incident has been properly contained
- Serves as the primary contact for the incident
- Ensures appropriate stakeholders are designated specific roles and responsibilities
- Includes additional resources and SPIRT virtual team members, as appropriate
- Leads the incident responders to consensus on taking action or making decisions during the incident
- Establishes out of band communication channels, as appropriate

The **incident coordinator** is responsible for the oversight of the incident response, including, but not limited to, the following duties:

- Coordinates all meetings, including place, time, attendees, conference bridges, etc.
- Aggregates documentation in a secured and centrally-stored facility (electronic/physical)
- Provides documentation related to the incident to the SPIRT core team
- Ensures adherence to this policy and any regulatory reporting requirements
- Ensures interview communication plans are established
- Establishes a response timeline

The **IT forensics investigator** is responsible for the electronic discovery of data from in-scope systems, applications, or logs. Other duties may include:

- Collect and preserve any physical evidence in a forensically-sound manner
- Adhere to appropriate chain of custody procedures
- Perform searches for various keywords, timelines, etc.
- Document any relevant findings and provide to the incident coordinator

The **data analysis investigator** is responsible for reviewing all aggregated documents, forms, transcripts, and other relevant materials. In addition, the data analysis investigator is responsible for the following duties:

- Validate the scope of the incident and possible root cause
- Establish the relevancy of all aggregated materials
- Collect materials from interviews, (e.g., transcripts, other artifacts, etc.) and presents to team for further review
- Quantify impact to WCM and other affected individuals
- Establish proof of the incident
- Prepare incident reports and a comprehensive narrative of the incident
- Prepare any necessary presentation materials

The **communications coordinator** must be prepared to respond to any authorized/approved party at any time throughout the incident. Responsibilities include:

- Maintain awareness of the incident status throughout the investigation
- Plan for controlled notifications to internal and external parties, including press releases, letters, website materials, or other notifications

6. Remediating an Incident

6.01 Maintaining Confidentiality

In order to limit exposure and maintain confidentiality about the incident, limited information pertaining to the incident should be disclosed upon initial notification (e.g., type/category of incident, date occurred, reported by, etc.). An informed parties log may be kept to document the degree and reason to which all parties have been informed about the incident.

Throughout all communications, the incident responders should be reminded of the confidentiality of the incident and that information must not be shared outside the response team unless warranted.

6.02 Incident Report

The initial incident report must be presented and reviewed at the convening of the SPIRT core team. The SPIRT data analysis investigator is responsible for compiling the data elements below as part of the incident response procedures. Appropriate templates are available based on the type of incident. Distribution and review of the working draft is restricted and must be conducted under privilege with a member of the Office of University Counsel included on any distribution list or at the review sessions. The incident report must contain the following attributes:

- Incident name
- Incident number
- Incident description and type
- Date and time declared
- Date and time discovered/reported
- Date and time occurred
- Date and time contained
- Date and time remediated
- Assets or systems involved
- Data involved, including data type, and independent verification
- Individual(s) involved
- Individual(s) affected
- Root cause analysis
- Containment steps and verification
- Comprehensive response steps/action log[1]
- Remediation steps[2]
- Communications plan[3]
- Regulatory reporting requirements[4]
- Lessons learned

Throughout the incident response process, all items should be completed, when known, before the report can be finalized.

[1] The action log must include all actions taken in chronological order, along with communications made and the indexing of any potential threats found, pertinent discoveries made, or potential data involved throughout the process.

[2] The remediation plan should eliminate, mitigate, or document acceptance of the threats discovered in the incident and any actions to address these items going forward.

[3] The communications plan must include the timing, preparation, revision, acceptance, and delivery of internal communications (e.g., executive committees, faculty, staff, students, affiliate institutions, etc.) and external communications (e.g., media, website, letters to affected individuals, etc.).

[4] Regulatory reporting and/or notification requirements, including deadlines, must be adhered to in accordance with applicable state, federal, or regulatory agencies (as described in 3.01 Identifying Affected Data).

7. Closing an Incident

Closing an incident indicates that the incident has been completely contained, remediated, and properly reported. In order to close an incident, all attributes in the incident report must be completed, as defined in Incident Report.

Incidents can only be closed by consensus of the SPIRT core team.

All documentation and evidence pertaining to the incident must be stored in a secure location approved by the Office of University Counsel. A paper copy of the incident report should be provided to and retained by the Office of University Counsel. The data analysis investigator should ensure that all documentation is organized in a clear, cohesive manner. It is important to note that additional activities may occur after the incident has been closed, such as responding to requests for additional information from regulatory agencies. These activities need to be memorialized and added to the documentation repository. Additionally, the SPIRT core team should be notified of any new developments, including regulatory inquiries, to closed incidents.

A post-mortem meeting should be held within ten business days to review the incident and adherence to this policy for any future modifications. An independent reviewer may be engaged to provide additional feedback on the incident handling procedures and records.