	WCM Administrative Policy and Procedure	
Weill Cornell Medicine	**Policy Title**	Security and Privacy Incident Response Plan
	Policy Number	ITS-500.05
	Department/Office	ITS Security
	Effective Date	October 1, 2007
	Last Reviewed	July 12, 2024
	Approved By	WCM-Executive Policy Review Group
	Approval Date	March 24, 2026

Purpose

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 WCM's compliance program.

This policy provides a framework for identifying, assessing, reacting to, communicating about, and documenting Significant Incidents, along with corresponding remediation plans.

This policy is specifically intended to govern high-impact privacy incidents and IT security incidents that may require coordinated institutional response, including activation of the Security & Privacy Incident Response Team (SPIRT). Routine privacy incidents are managed in accordance with the Office of Compliance (OOC) policies and procedures and do not require SPIRT activation unless escalation criteria are met.

Scope

This policy applies to all WCM Workforce Members who utilize WCM information technology resources as well as those responsible for managing and safeguarding WCM data.

Policy

All WCM Workforce Members are responsible for protecting the confidentiality, integrity, and availability of data created, received, stored, transmitted, or otherwise used by WCM, irrespective of the medium on which the data resides and regardless of format.

In the event the confidentiality, integrity, or availability of data is compromised, ora suspected incident has occurred, the incident must be reported immediately to the Information Technologies & Services Department (ITS) and/or the OOC, as appropriate.

All suspected incidents must be reported; however, only incidents meeting defined severity and impact thresholds (e.g., large-scale data exposure, system compromise, ransomware, regulatory reporting triggers, or significant reputational risk) will be escalated for formal declaration and potential SPIRT activation.

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.

Definitions

Low-Scale Security Incidents: This is an incident that requires internal investigation and attention but doesn't rise to the level of a breach or crisis because it could signal a gap in process, awareness, or configuration. For example, an individual's credentials are compromised without exposing sensitive data. Another example is a policy violation without data exposure, such as using unlicensed software on a WCM-owned and managed endpoint.

Protected Health Information (PHI): Under HIPAA, PHI is "individually identifiable health information" held, created, or transmitted by a covered entity, or its business associate, in any form or media, whether electronic, paper, or verbal.

A. PHI is information, including demographic data, related to:
    a. The provision of health care to an individual; or
    b. An individual's past, present, or future:
        1. physical or mental health condition; or
        2. payment for the provision of health care to an individual; and
B. The information identifies the individual or there is a reasonable basis to believe the information can be used to identify the individual by the presence of one or more (depending on the context) of the following 18 individual identifiers:
    1. Names;
    2. Geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP code, and their equivalent geocodes, except for the initial three digits of a ZIP code in certain situations;
    3. All elements of date (except year) for dates directly related to an individual, including birth date, discharge date, date of death; and all ages over 89 and all elements of dates indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
    4. Telephone numbers;
    5. Fax numbers;
    6. Electronic mail addresses;
    7. Social Security numbers;
    8. Medical record numbers;
    9. Health plan beneficiary numbers;
    10. Account numbers;
    11. Certificate/license numbers;
    12. Vehicle identifiers and serial numbers, including license plate numbers;
    13. Medical device identifiers and serial numbers;
    14. Web Universal Resource Locators (URLs);
    15. Internet Protocol (IP) address numbers;
    16. Biometric identifiers, including finger and voice prints;
    17. Full face photographic images and any comparable images; and
    18. Any other unique identifying number, characteristic, or code unless otherwise permitted by this Policy for re-identification (§164.514(b)(2)).

Significant Incidents: An event involving the actual or suspected compromise of data confidentiality, integrity, or availability that meets one or more of the following criteria:

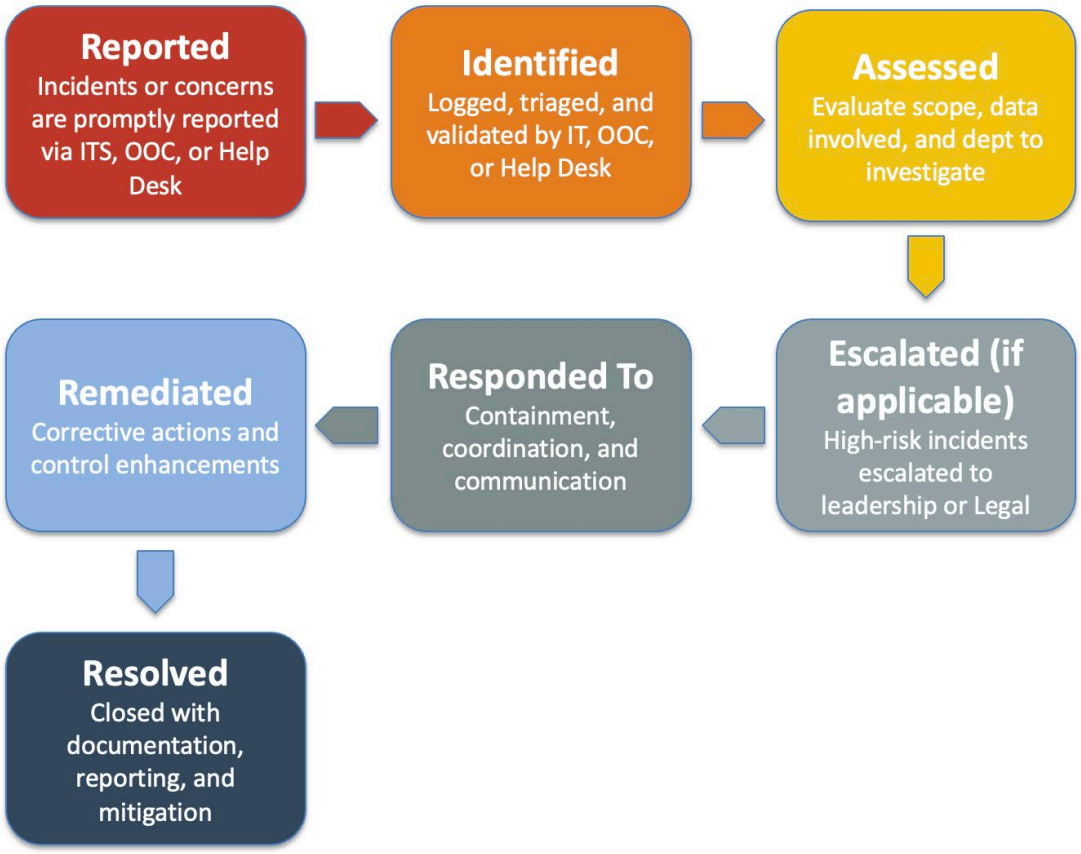
- Large volume of sensitive data (e.g., PHI, PII, financial data)
- Confirmed or suspected system intrusion, malware, or ransomware
- Regulatory reporting or notification obligations
- Material operational disruption
- High reputational or legal risk to WCM
- Intentional wrongdoing/theft of data by Workforce Member(s)

Routine Privacy Incident: Lower-risk incidents (e.g., misdirected fax/email, limited disclosure, minor documentation errors) that are investigated and managed by the OOC and do not require SPIRT activation unless escalation criteria are met.

Workforce Members: Faculty; Non-Faculty Academics; Staff; Students; Volunteers; and other persons whose conduct, in the performance of work for WCM, is under the direction and control of WCM, whether or not they are paid by WCM.

Procedure

Security and privacy incidents should be (1) reported, (2) identified, (3) assessed, (4) escalated (5) responded to, (6) remediated, and (7) resolved with adequate record-keeping. Detailed requirements for each of these steps are below.



1. Reporting an Incident

If you know or suspect any unusual or suspicious behavior, immediately report the incident to ITS Support or the OCC. Even if you are not certain or cannot confirm the incident, it's imperative that the incident is reported timely so the right personnel can investigate as soon as possible, however, reporting does not automatically trigger SPIRT activation.

To report an incident, notify ITS Support:

ITS Support
Telephone: (212) 746-4878
Email: support@med.cornell.edu

ITS Security
Telephone: (646) 962-3010
Email: its-security@med.cornell.edu

ITS Support (Qatar)
Telephone: +974 (4492) 8711
Email: its-alert@qatar-med.cornell.edu

Office of Compliance
Telephone (Compliance): (646) 962-7539
Email: compliance@med.cornell.edu
Telephone (Privacy): (646) 962-6930
Email: privacy@med.cornell.edu

Cornell University Hotline (Anonymous)
Telephone: (866) 293-3077
Website: https://audit.cornell.edu/services/ethical-conduct-and-compliance-hotline/

Compliance Office (Qatar)
Telephone: +974 (4492) 8807
Email: grc@qatar-med.cornell.edu

ITS (Qatar) Anonymous
Email: its-anonymous@qatar-med.cornell.edu

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

Examples of reportable incidents include, but are not limited to the following:

- Misplaced, stolen, or lost devices containing WCM data
- 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 a victim of malware, phishing, or ransomware events
Note: Not all incidents listed above constitute a “Significant Incident.” Many may be managed as routine privacy or operational incidents unless escalation criteria are met.

2. Identifying an Incident

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

A. Routine Privacy Incident (managed by the OOC)
B. IT Security Incident (managed by ITS Security)
C. Significant Incident (requires escalation and potential SPIRT activation, Managed by ITS/OOC depending on the nature of the incident)

2.01 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 WCM. This also includes the evaluation of the state of residence for affected individuals and any applicable reporting authorities. For Significant Incidents, regulatory reporting requirements must be evaluated and managed in coordination with SPIRT and the Office of General Counsel.

Refer to WCM Policy OOC-410.05 – *HIPAA and State Privacy Breach Notifications* for additional requirements related to breach notification and reporting.

3. Declaring an Incident

The Chief Information Officer, the Chief Information Security Officer, the Chief Compliance and Privacy Officer, or their designees may declare a significant privacy and/or IT security incident. These individuals are responsible for evaluating the reported concern using the tools and risk assessment guides to determine the concern's authenticity and severity. Severity judgments will be based on ongoing persistent threats, the volume of data involved, and the potential for reputational or financial harm to the institution or affected individuals.

Low-Scale Security Incidents and Routine Privacy Incidents should be handled by the appropriate ITS team or the OOC. Routine privacy incidents will not be declared under this policy and will instead follow established workflows in the OOC.

Only incidents, determined to be "Significant Incidents" will be formally declared and considered for SPIRT activation These include, but are not limited to:

- Confirmed or suspected cyberattack (e.g., ransomware, system compromise)
- Large-scale breach of PHI or sensitive data
- Incidents requiring regulatory notification
- Events with enterprise-wide operational or reputational impact

The primary purpose of SPIRT is to determine and guide the WCM's response to Significant Incident, up to and including the need to satisfy existing data breach notification requirements or processes as well as an institutional decision to notify individuals of a breach of their information.

The SPIRT core team members include:

1. Chief Information Officer
2. Chief Information Security Officer
3. Chief Compliance and Privacy Officer
4. Associate Vice President, Deputy General Counsel and Secretary
5. Assistant Vice Provost, Communications & Public Affairs

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. Assistant Vice Provost, Human Resources
6. Department Administrator II, Graduate School
7. Associate Director, Medical Education Administration
8. Chief Medical Officer
9. Chief Medical Information Officer
10. Controller
11. Chief Information Security Officer, Cornell University
12. Chief Audit Executive, Cornell University
13. Chief Information Officer (Weill Cornell Medicine-Qatar)
14. Vice President, Chief Information Security Officer (NewYork-Presbyterian Hospital)
15. Chief Information Security Officer (Columbia University Irving Medical Center)
16. Chief Privacy Officer (NewYork-Presbyterian Hospital)
17. Chief Privacy Officer (Columbia University Irving Medical Center)
18. 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.

4. Coordinating a Response to an Incident

These procedures apply to Significant Incidents requiring SPIRT activation.

4.01 Containing the Incident

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

- For IT security-related incidents, such as an infected system on the WCM network, network connections should be disabled, and the system should remain powered on but not used 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.

4.02 Assigning Roles

Upon declaring the incident, the SPIRT core team members may 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 for 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:

- Collects and preserves any evidence in a forensically-sound manner
- Adheres to appropriate chain of custody procedures
- Performs searches for various keywords, timelines, etc.
- Documents 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:

- Validating the scope of the incident and possible root cause
- Establishing the relevancy of all aggregated materials
- Collecting materials from interviews, (e.g., transcripts, other artifacts, etc.) and presents to team for further review
- Quantifying impact to WCM and other affected individuals
- Establishing proof of the incident
- Preparing incident reports and a comprehensive narrative of the incident
- Preparing 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:

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

5. Remediating an Incident

5.01 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 documenting the degree and reason to which all parties have been informed about the incident.

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

5.02 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 General 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 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
- Date and time declared
- Date and time discovered/reported
- Date and time occurred
- 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 should 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 should include the timing, preparation, revision, acceptance, and delivery of internal communications (e.g., shared governance bodies, 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, shall be adhered to in accordance with applicable state, federal, or regulatory agencies (as described in 2.01 Identifying Affected Data and WCM Policy OOC-410.05 - *HIPAA and State Privacy Breach Notifications*).

6. 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 5.02 Incident Report.

Only SPIRT-managed Significant Incidents require formal closure by the SPIRT core team.

Routine incidents are closed in accordance with the OOC procedures.

All documentation and evidence and the incident report pertaining to the incident must be stored in a secure location by the Chief Information Security Officer. A paper copy of the incident report should be provided to the Office of General 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 for Significant Incidents 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.

Compliance with this Policy

All WCM Workforce Members are responsible for adhering to this policy. Failure to comply will be evaluated on a case-by-case basis and could lead to corrective action, up to and including termination, consistent with other relevant WCM and University Policies. Instances of non-compliance that potentially involve a lapse of professionalism may lead to engagement of the Office of Professionalism for evaluation and intervention.

Contact Information

Direct any questions about this policy, ITS-500.05 – Security and Privacy Incident Response Plan, to the Chief Information Security Officer, using one of the methods below:

- Office: (646) 962-3609
- Email:ciso@med.cornell.edu

References

- WCM Policy OOC-410.05 - HIPAA and State Privacy Breach Notifications

Policy Approval

This policy was reviewed and approved by:

- Information Security and Privacy Advisory Committee (ISPAC) on March 19, 2026.
- WCM-Executive Policy Review Group (WCM-EPRG) on March 24, 2026.

Version History

Date	Author	Revisions
10/01/2007		Policy implemented
11/08/2018	Brian J. Tschinkel	Modified membership roles and breach notification requirements
11/12/2020	Brian J. Tschinkel	Modified membership roles
02/08/2022	Brian J. Tschinkel	Recertified policy
02/09/2023	Brian J. Tschinkel	Recertified policy and updated membership titles
03/14/2023	Brian J. Tschinkel	Minor grammatical updates and membership title changes
07/02/2024	Tom Horton	Title changes and contact information
07/12/2024	Christine Klucznik	Updated policy template and language
03/24/2026	Office of the CISO	Updated policy template and language

Appendix

N/A