Weill Cornell Medicine

11.19

Security Compliance Workforce Training and Education

Responsible Executive: Chief Information Security Officer, Weill Cornell Medicine
Original Issued: March 17, 2022
Last Updated: September 6, 2023
Last Reviewed: September 6, 2023

Contents

Policy Statement

Weill Cornell Medicine is required to train and/or educate all workforce members on security policies and best practices. Training content will address Weill Cornell Medicine policies and procedures, safeguards to comply with regulatory requirements, and other industry best practices to reduce the likelihood of a breach of confidentiality, integrity, or availability of information assets.

Reason for Policy

Security awareness training helps educate workforce members to better detect threats and suspicious activity. Increasing awareness around common security threats helps reduce the likelihood of a breach of Weill Cornell Medicine data. The content within these training courses is designed to comply with legal and regulatory standards, including but not limited to the Health Insurance Portability and Accountability Act (HIPAA) and the Payment Card Industry Data Security Standard (PCI DSS).

Entities Affected by this Policy

All Weill Cornell Medicine workforce members. *Workforce Member*, as defined in Compliance and Privacy Office policy *HIPAA Compliance Workforce Training & Education*, includes “any faculty, staff, students, volunteers, trainees, and other persons whose conduct, in the performance of work for Weill Cornell Medicine, is under the direction and control of Weill Cornell Medicine, whether they are paid by Weill Cornell Medicine.”

Who Should Read this Policy

All members of the Weill Cornell Medicine community utilizing Weill Cornell Medicine information technology resources. All stewards and custodians of Weill Cornell Medicine data.

Web Address of this Policy

https://its.weill.cornell.edu/policies

Contacts

Direct any questions about this policy, 11.19 – Security Compliance Workforce Training and Education, to Brian J. Tschinkel, Chief Information Security Officer, using one of the methods below:

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

1. Individual Responsibilities

All WCM workforce members are expected to comply with the mandatory training requirements defined in this policy. Department administrators, including Chief Administrative Officers, are expected to ensure that no workforce member is delinquent with mandatory security awareness training.

2. Required Training Courses

2.01 ITS Phishing Awareness Training Course

This phishing awareness training course tests the ability to identify, analyze, and detect suspicious email messages. The course includes a series of exercises to test proficiency and informs workforce members on how to report suspicious messages to ITS.

This course must be completed within forty-five (45) calendar days of hire or affiliation. Access to Weill Cornell Medicine systems may be impacted if the course is not completed within this period. This course is accessible in Weill Business Gateway using the Learning tile.

2.02 ITS High Risk Attestation

This attestation records if workforce members work with, or could reasonably be exposed to, protected or regulated data, including protected health information (PHI), personally identifiable information (PII), and other high risk data pursuant to ITS policy 11.03 – Data Classification. These data are termed high risk because of the harm that loss of the data could cause to the subject of the data, to workforce members, and to the institution if it not protected adequately.

Workforce members are asked to provide an inventory of the devices they use for regularly storing or accessing Weill Cornell Medicine high risk data. Based on their level of exposure to high risk data, workforce members are asked to attest to a series of statements about safeguarding this data in compliance with Weill Cornell Medicine policies and procedures.

The ITS High Risk Attestation must be completed within forty-five (45) calendar days of hire or affiliation and annually thereafter. Access to Weill Cornell Medicine systems may be impacted if the course is not completed within this period. The course is accessible at https://attest.weill.cornell.edu.

3. Training Frequency & Delivery Methods

3.01 Upon Hire or Affiliation

All newly recruited Weill Cornell Medicine workforce members are required to complete security awareness training courses within forty-five (45) calendar days of hire. In addition to the courses identified in the previous section, an overview of security topics is provided at new employee orientation and in the HIPAA training courses administered by the Compliance & Privacy Office.

3.02 Annual Update Training

All Weill Cornell Medicine workforce members must complete required “update” courses on an annual basis to keep current and ensure compliance with relevant requirements. Access to Weill Cornell Medicine systems may also be impacted if mandatory “update” courses are not completed within the deadline.

3.03 Phishing Exercises

The ITS Security team may conduct phishing awareness campaigns to measure the effectiveness of the Weill Cornell Medicine community in identifying phishing attempts and to assist with developing additional training content. These phishing awareness campaigns may be conducted at any time throughout the year.

3.04 Ad Hoc Training

Additional security awareness training may be required at the discretion of the Chief Information Security Officer, in response to a security incident, or in response to new policies, processes, procedures, and/or technologies.

Upon request of department administration, additional training may be delivered by the ITS Security team to a department, division, office, or site, and this training will be customized to topics of interest.

Other course content may be curated by ITS Security and made available for voluntary completion at https://phish-camp.weill.cornell.edu.

4. Non-compliance with Security Awareness Training

ITS Security reserves the right to restrict access of any Weill Cornell Medicine workforce member who fails to complete mandatory security awareness training requirements within the required period. The following sanctions may be imposed:

- The individual's access to Weill Cornell Medicine systems, including Epic, may be disabled.
- The individual's access to Weill Cornell Medicine email may be disabled.
- The individual's supervisor, department administrator, or chairperson may be notified.

Human Resources, Office of General Counsel, Compliance and Privacy Office, or any other relevant administrative unit may be involved for correction action, if necessary.

Upon satisfactory completion of mandatory security awareness training courses, all access will be restored.

Revision History:

Date	Author	Revision
March 14, 2022	Justin Barber, Brian J. Tschinkel	Initial draft completed
March 17, 2022	Brian J. Tschinkel	Approved by Information Security & Privacy Advisory Committee (ISPAC)
September 6, 2023	Brian J. Tschinkel	Updated policy template to conform with branding