FY24 Information Security Compliance Plan

Mission Statement

The mission of The University of Texas MD Anderson Cancer Center (MD Anderson) is to eliminate cancer in Texas, the nation, and the world through outstanding programs that integrate patient care, research, and prevention, and through education for undergraduate and graduate students, trainees, professionals, employees, and the public.

To fulfill this mission:

- We are committed to meeting the highest standards of medical, research, and business ethics.
- We recognize that, regardless of payor source, appropriate, medically necessary services must be delivered in the most efficient manner and meet all applicable local, state, and federal guidelines and regulations.
- We understand that promoting research integrity, including appropriate use of all research funding and accurate documentation of all research work, is critical to ensuring our ongoing research efforts and fulfilling federal, state, and UT System requirements.
- We are intolerant of fraud, waste, abuse, and other violations of such guidelines and regulations.
- We are committed to providing education, monitoring, and oversight to ensure that faculty, employees, volunteers, trainees, contractors, and other persons whose conduct, in the performance of work for MD Anderson, is under the direct control of MD Anderson, whether or not they are paid by MD Anderson (collectively referred to as Workforce Members), are fully informed and committed to these standards.
- We facilitate programs to address key risk areas including international relationships, cybersecurity threats, and continually reassess the risk environment to proactively develop standards and processes that protect our resources.
- We promote an open work environment so that all individuals associated with MD Anderson feel free to communicate openly on such issues.

The mission of MD Anderson's Institutional Compliance Program is to support MD Anderson's mission, vision and core values and to help the institution fulfill its responsibilities to the people of Texas in an environment based upon ethical behavior and compliance with applicable laws, rules, and guidelines.

To that end, the Institutional Compliance Program will:

- Provide all workforce members with the most accurate, concise, and up-to-date information and advice to assure awareness of their responsibilities with respect to sustaining such an environment;
- Foster an environment of open communication by educating workforce members about their obligations to report compliance concerns;

- Protect workforce members from retaliation if they, in good faith, report suspected wrongdoing, participate in or with an institutional investigation pertaining to alleged wrongdoing, or assist appropriate authorities in investigating possible wrongdoing; and
- Continually assess the effectiveness and quality of its program to ensure all MD Anderson business is conducted with integrity and in compliance with the law.

Code of Conduct

MD Anderson requires all administration staff, medical staff, employees, and other workforce members to follow the **Standards of Conduct** adopted by the Board of Regents.

MD Anderson is committed to full compliance with all applicable laws, rules, and guidelines. To such end and in order to uphold MD Anderson's core value of Integrity, our workforce members are required to conduct themselves in accordance with the ten principles comprising **MD Anderson's Code of Conduct**:

Know and follow the rules

Know and follow the letter and the spirit of applicable laws, rules, and guidelines, as well as UT System and MD Anderson rules, policies, procedures, and compliance plans.

Think and act ethically

Follow our ethical standards and those of your professional organizations. Before you say or do something, ask yourself: How would this look to our patients and our community? Would this harm our reputation?

Keep it confidential

Handle all MD Anderson information, especially patient information, in ways that meet applicable laws, rules, guidelines, and document retention schedules. Treat our information the same way you treat yours.

Commit to research integrity

Perform all research efforts in ways consistent with applicable legal, ethical and professional requirements, as well as MD Anderson rules, policies and procedures.

Avoid gifts

In general, you can't accept or give gifts, favors, benefits, services, or items of value — especially in return for preferential treatment or patient referrals.

Bill accurately

When you document and bill for the care you've provided, be accurate, be thorough, be honest — and be timely.

Focus on Making Cancer History

Don't use any MD Anderson resources, including your time and your colleagues' time, in a wasteful manner, for personal benefit, to harm someone, for political activity, or for illegal activity.

Be true to our mission: Avoid outside influences

Don't engage in activities or enter into contracts that could or could seem to interfere with your MD Anderson work, make you disclose confidential MD Anderson information, or affect your independent judgment.

Be a good colleague

Act with honesty and good faith in all matters. Don't engage in discriminatory, harassing, retaliatory, inappropriate, intimidating, or disruptive behaviors

When in doubt, point it out

If you think or discover that someone isn't following our Code of Conduct, promptly notify the Chief Compliance and Ethics Officer or Institutional Compliance. And always cooperate fully with all inquiries and investigations related to reported issues.

Information Security Compliance Oversight

The purpose of the Information Security Compliance Plan is to serve as the governing document for MD Anderson's means of insuring effective information security compliance in a manner consistent with MD Anderson's Mission Statement, Institutional Code of Conduct, and Hospital Compliance Plan.

Responsibility for oversight of the Compliance Plan rests with a multi-disciplinary Information Security Compliance Committee (ISCC), whose membership is appointed by the Vice President, Chief Compliance and Ethics Officer (CCEO) and annually approved by the Executive Institutional Compliance Committee (EICC). This is consistent with the governance structure recommended in National Institute of Standards and Technology (NIST) Special Publication 800-39, Managing Information Security Risk: Organization, Mission, and Information System View. All members of the ISCC must sign a statement assuring total confidentiality in all dealings of the ISCC. The ISCC is a Medical Committee within the meaning of Texas Health and Safety Code § 161.031. Minutes of all ISCC meetings are maintained in a confidential manner and are provided to the EICC. Minutes are maintained in the Institutional Compliance Office.

The Science, Technology and Research Compliance Committee (STARCC), a subcommittee of the ISCC, is responsible for promoting the security of information, resources, and other products resulting from research efforts led or supported by MD Anderson. STARCC composition, functions, and responsibility information is described in its bylaws.

The ISCC is charged with the following tasks:

- Prepare and submit to the EICC an annual work plan that outlines the major activities and initiatives of the ISCC for the upcoming fiscal year.
- Prepare and submit to the EICC an annual report that summarizes the ISCC's progress regarding each work plan objective contained in the ISCC's annual work plan for the preceding fiscal year.
- Validate the annual Compliance Risk Analysis related to information security compliance matters.

The responsibility for implementing and managing the Institutional Compliance Program and Information Security Compliance Plan is assigned to the CCEO, who functions within MD Anderson's organizational structure with a direct reporting relationship to the President and an administrative reporting relationship to the Senior Vice President, Regulatory Affairs. . The CCEO, or designee, will, with assistance of the ISCC, perform the following activities:

- Review the laws, regulations, statutes, policies and guidelines related to information security and, in particular, protection of information resources from unauthorized data disclosure and data loss.
- Recommend the creation of new information security policies as well as revisions to current security policies and

procedures to the ISCC for approval.

- Organize and lead the implementation of new and revised information security policies and procedures.
- Develop and monitor practical methodologies and systems to optimize information security compliance.

- Develop and implement necessary changes in practices or procedures that assure adherence to established information security compliance policies.

- Propose revisions, on an as-needed basis, to all related information security policies and procedures for approval by the respective parties.

Education

Compliance with all applicable laws and regulations is one of MD Anderson's priorities. Workforce Members at MD Anderson must be knowledgeable about MD Anderson's Institutional Code of Conduct, Standard of Conduct: Do the Right Thing and policies and plans regarding institutional compliance issues. Compliance with applicable laws, rules, guidelines, as well as institutional policies and plans is a condition of employment. Failure to comply may result in disciplinary action, including termination.

In addition, the CCEO, with the assistance of the Information Security Compliance Committee, is responsible for education and training programs related to the Information Security Compliance Plan. The CCEO or designated responsible parties may make attendance at these programs mandatory and may include such topics as:

- General information security compliance and best practices;

- Newly adopted, revised and established MD Anderson policies and procedures regarding information security;

- Implications of failing to adhere to the Information Security Compliance Plan and all applicable requirements;

- The Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009, and all relevant amendments and enacting regulations, Texas privacy law and other relevant legal requirements;

- Emerging regulatory compliance issues;

- Training on specific risk areas;

- Implication of the Institutional Compliance Program and the Information Security Compliance Plan on job requirements and as part of the employee's annual evaluation;

- Implementation of **UTMDACC Institutional Policy #ADM0335, Information Security Office Policy for the Use and Protection of Information Resources; UTMDACC Institutional Policy #ADM1187, Electronic Confidential and Restricted Confidential Information Access and Storage Policy, and UTMDACC Institutional Policy #ADM1188, Use of Personally-Owned Mobile Devices for Institutional Use Policy**; and

- Implementation **of The University of Texas System Policies & Standards UTS165: Information Resources Use and Security Policy (UTS165).**

A variety of teaching materials, tools, and methods are used as necessary. Ongoing education is provided as appropriate to review information security issues and to inform employees on new and emerging information security areas. The Institutional Compliance Office maintains records, including attendance logs and presentation materials, related to its education and training sessions. Failure to comply with the education requirements may lead to disciplinary actions, as provided for by MD Anderson's Corrective Action Policy (UTMDACC Institutional Policy # ADM0256).

Ongoing Monitoring and Auditing

1.0 Monitoring Activities

1.1 The CCEO, or designee, shall meet periodically with designated departmental representatives to stay abreast of current and/or new matters related to information security compliance.

1.2 The CCEO, or designee, shall monitor the progress of risk management plans.

2.0 Auditing Activities

The CCEO, or designee, shall perform periodic audits or similar assurance activities regarding information security compliance

Investigation and Remediation

Institutional Compliance investigations are conducted under, and therefore protected by, one or more of the following: Texas Rule of Evidence 503 (the lawyer-client privilege), Texas Education Code §51.971 (institutions of higher education conducting compliance program investigations), and/or Texas Health and Safety Code §161.032(b)(1), (c), and (e) (Medical Committees and compliance officer privileges).

The CCEO, with support from legal counsel and the EICC, addresses any violation of the laws, regulations, and institutional policies and standards applicable to governmental compliance. Whenever a compliance concern has been raised through MD Anderson's Compliance Hotline, direct contact, a third-party, or any other source, and a preliminary assessment suggests that an investigation is warranted, the CCEO will initiate a confidential investigation to determine the facts and circumstances of the potential violation. Compliance investigations will involve only those individuals necessary to resolve a fact or issue. Barring exceptional circumstances, the CCEO does not apprise complainants or reporters of the status of investigations.

The CCEO may accept a previously conducted investigation if such investigation was conducted with knowledge and approval of the CCEO. Compliance investigations will be performed with the assistance of legal counsel and MD Anderson subject matter experts, as needed, and will be reported immediately and confidentially to the EICC, as appropriate. If the CCEO believes the integrity of the investigation is at stake, the appropriate workforce member(s) may be removed from duty until the investigation is completed. The CCEO ensures that steps are taken to prevent destruction of documents or other evidence.

The CCEO promptly and fully investigates all reports professionally and without prejudice. Consultations follow with the appropriate division head(s), department chair(s), manager(s), and/or workforce member(s), as appropriate.

The CCEO ensures that all those interviewed as part of the investigative process are entitled to have a representative/advocate present during their interview. However, an interviewee's representative or advocate is not permitted to steer, coach, or rehabilitate the interviewee's responses or otherwise compromise the integrity of the interview. Any such attempts to compromise the integrity of the interview may considered noncooperation. The interviewee will be provided with a copy of MD Anderson's Non-Retaliation Policy (MD Anderson Institutional Policy #ADM0254) and apprised of the ramifications of, as a consequence of the interview, engaging in conduct implicated by the Policy.

If an investigation indicates that corrective action is warranted, such action will be imposed in accordance with MD Anderson's written standards of corrective action, and outlined in a corrective action plan. The corrective action plan to be implemented is developed after the outcome of an investigation. In determining the corrective action plan, MD Anderson should not take into consideration a workforce member's economic or reputation benefit to the institution. All corrective actions provided in the plan are disseminated to those responsible for completing such actions, and must be undertaken and completed within their specified time frames.

Any misconduct that violates civil or criminal law, rules or regulations may be reported to the appropriate governing body after receipt of credible evidence of such misconduct, along with a description of the appropriate corrective action taken. If applicable, plans for repayment of federal funds will be included in the report.

Corrective action plans also should include determining whether the problem is systemic and implementing any necessary preventive measures.

Corrective and/or Disciplinary Action

MD Anderson upholds a zero tolerance policy toward any illegal activity or knowing, willing, or intentional noncompliance with federal and state laws and regulations, and MD Anderson's policies. All actions taken will be in accordance with MD Anderson's **Hospital Compliance Plan**.

Sanctioned Individuals

MD Anderson prohibits the employment of individuals who:

- have a criminal history related to federal health care program or state health care program; or
- have been disbarred, excluded, or otherwise determined ineligible for participation in federal health care programs as evidenced by appearance in one of the following agencies (Adverse Action Databases") Sanction Checks are handled in accordance with the MD Anderson **Hospital Compliance Plan**.

Reporting Compliance Concerns

Remaining silent and failing to report any violation or potential violation that a workforce member knows or should have known of may subject a workforce member to corrective action up to and including termination. MD Anderson will not accept workforce member's claim that improper conduct occurred for the benefit of MD Anderson. Any such conduct is not for the benefit of MD Anderson and is expressly prohibited.

To encourage open communication in all dealings with the CCEO and the EICC, workforce members contacting Institutional Compliance are assured non-retaliation in accordance with the **Non-Retaliation Policy (MD Anderson Institutional Policy #ADM0254)** and an atmosphere of confidentiality.

To report compliance concerns, workforce members and any other member of the MD Anderson community, including patients and their family members, may:

- Call the Compliance Hotline at 1-800-789-4448;
- Call Institutional Compliance directly at 713-745-6636; or
- Contact the CCEO via the Page Operator at 713-792-7090.
- Email Institutional Compliance at **Institutional_Compliance@mdanderson.org**; or
- Submit an online report through the **Detecting and Addressing Compliance Concerns webpage**

Suspected fraud, waste, and abuse involving state resources may be reported to the State Auditor's Office's Hotline at 1-800-TX-AUDIT (1-800-892-8348). The State Auditor's Office provides additional information at its website.

MD Anderson has established the Compliance Hotline, listed above, for workforce members and other members of the MD Anderson community to report all suspected violations or questionable conduct. The Compliance Hotline includes the following features:

- The Compliance Hotline number is included in employment materials, employee badge cards, the Institutional Compliance Program website, MD Anderson's Standards of Conduct: Do the Right Thing, and is displayed in poster form on MD Anderson bulletin boards;
- Telephone calls to the Compliance Hotline are treated anonymously, upon request, and confidentially to the extent possible;
- The caller is not recorded, traced or identified, and the caller is not required to furnish their name;
- Information provided to the Compliance Hotline is treated as privileged to the extent permitted by applicable law;
- Upon receiving information from the Compliance Hotline, the CCEO will communicate and disseminate all compliance complaints to the triage team and assign to the appropriate party for investigation;
- Each report will be reviewed, and the CCEO or designee will initiate any investigations, corrections and/or follow-up on an as-needed basis in accordance with provisions of this plan; and,
- The CCEO will provide routine reports and periodic updates as deemed necessary to the EICC and President.

Note that intentionally making false accusations is a serious violation of MD Anderson policy and may lead to corrective actions against the person making the accusation, up to and including termination of employment. Workforce members may not use the Compliance Hotline to protect themselves from the outcome of their own violations or misconduct; however, self-reporting is strongly encouraged and may be considered a mitigating factor when determining the appropriate corrective actions.

In all reports of compliance concerns, the CCEO strictly complies with and enforces MD Anderson's **Non-Retaliation Policy (MD Anderson Institutional Policy #ADM0254)**.

References

Terms not defined in the Information Security Compliance Plan are contained in MD Anderson's HIPAA **Definition Plan.**

Corrective Action Policy (MD Anderson Institutional Policy #ADM0256)

Hospital Compliance Plan

Non-Retaliation Policy (MD Anderson Institutional Policy #ADM0254)

MD Anderson's Standards of Conduct

State Auditor's Office

Texas Health and Safety Code § 161.031

http://sao.fraud.state.tx.us

The University of Texas System Policies & Standards - UTS165: Information Resources Use and Security Policy (UTS165).

Information Security Office Policy for the Use and Protection of Information Resources (UTMDACC Institutional Policy #ADM0335)
Electronic Confidential and Restricted Confidential Information Access and Storage Policy (UTMDACC Institutional Policy #ADM1187)

Use of Personally-Owned Mobile Devices for Institutional Use Policy (UTMDACC Institutional Policy #ADM1188)

NIST SP 800-39 - Managing Information Security Risk - Organization, Mission, and Information System View

NIST SP 800-53, Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations

APPROVALS

Date	Approver
10-24-2023	Executive Institutional Compliance Committee
10-18-2022	Executive Institutional Compliance Committee
10-26-2021	Executive Institutional Compliance Committee
10-27-2020	Executive Institutional Compliance Committee
10-22-2019	Executive Institutional Compliance Committee
10-17-2018	Executive Institutional Compliance Committee
11-06-2017	Executive Institutional Compliance Committee
11-20-2014	Executive Institutional Compliance Committee
01-16-2014	Executive Institutional Compliance Committee
10-09-2012	Executive Institutional Compliance Committee
09-07-2011	Executive Institutional Compliance Committee

Content Experts:
Weber, Max C., Vice President & Chief Compliance and Ethics Officer
Bourgeois, Matt, Senior Legal Officer & Director