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 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 are intolerant of fraud, waste, and abuse and 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 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 MD Anderson Workforce Members with the most accurate, concise, and up-to-date information and advice to assure that they are aware of their responsibilities with respect to sustaining such an environment. The Institutional Compliance Program will also continually assess the effectiveness and quality of the program to ensure that all MD Anderson business is conducted with integrity and in compliance with the law.

CODE OF CONDUCT

MD Anderson requires all Administration, 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 following principles of the Institutional Code of Conduct:
Principle One: 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.

Principle Two: 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?

Principle Three: 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.

Principle Four: Commit to research integrity

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

Principle Five: 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.

Principle Six: Bill accurately

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

Principle Seven: 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.

Principle Eight: 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.

Principle Nine: 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.

Principle Ten: 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 the Institutional Compliance Office. And always cooperate fully with all inquiries and investigations related to reported issues.

COMPLIANCE OVERSIGHT

The purpose of the Privacy Compliance Plan is to:
• Ensure that all Protected Health Information ("PHI") will be managed with the highest levels of caring and integrity; appropriate permission is obtained for any uses and/or disclosures of PHI; and that only the minimum necessary PHI will be used and/or disclosed for each purpose.

• Inform both patients and Workforce Members of privacy issues and of everyone's role in the culture of privacy.

• Provide appropriate methods for patients, patient representatives, employees, contractors, and volunteers to discuss and communicate privacy concerns or questions with MD Anderson.

• Provide ongoing education, monitoring, and oversight to ensure that all workforce members are informed of the institution's requirements regarding patient privacy.

• Promote a work environment that allows open communication and swift resolution of any instances of violations of relevant guidelines and regulations.

Responsibility for oversight of the Privacy Compliance Plan rests with a multi-disciplinary Privacy Compliance Committee (PCC), whose membership is appointed by the Vice President, Chief Compliance and Ethics Officer (CCO) and annually approved by the Executive Institutional Compliance Committee (EICC). All members of the PCC must sign a statement assuring total confidentiality in all dealings of the PCC. Minutes of all PCC meetings are maintained in a confidential manner and are provided to the EICC. Minutes are maintained in the Institutional Compliance Office.

The PCC 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 PCC for the upcoming fiscal year.

• Prepare and submit to the EICC an annual report that summarizes the PCC’s progress regarding each work plan objective contained in the PCC’s annual work plan for the preceding fiscal year.

• Validate the annual Compliance Risk Analysis related to privacy compliance matters.

The responsibility for implementing and managing the Institutional Compliance Program and Privacy Compliance Plan is assigned to the CCO, who is the institution's Chief Privacy Officer and functions within MD Anderson's organizational structure. The CCO, or designee, will, with assistance of the PCC, perform the following activities:

• Review the laws, regulations, statutes, policies and guidelines related to privacy.

• Recommend the creation of new and revisions to current privacy policies and procedures to the Privacy Compliance Committee for approval.

• Organize and lead the implementation of new and revised privacy policies and procedures.

• Develop and monitor practical methodologies and systems to optimize privacy compliance.

• Develop and implement necessary changes in practices or procedures that assure adherence to established privacy policies.

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

• Develop and implement an educational training program for the Institution to ensure the understanding of federal and state laws and regulations involving ethical and legal business practices impacting privacy.
• Develop or assist with developing monitoring plans for high risk areas identified through the Compliance Risk Analysis.

• Conduct and coordinate the investigation of alleged privacy violations.

• Conduct physical safeguard audits.

• Handle inquiries by employees and patients regarding any aspect of privacy.

• Communicate regularly with the EICC on new and emerging issues.

• Notify requisite parties (e.g., patients, Office for Civil Rights (OCR), etc.) when unsecured PHI is breached, and submit an annual report of breaches to the OCR.

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

• General privacy compliance and best practices;

• Uses and/or disclosures of patient health information, and the required patient and/or statutory permissions for each purpose;

• Newly adopted, revised and established MD Anderson policies and procedures regarding privacy;

• Implications of failing to adhere to the Privacy Compliance Plan and all applicable health care program requirements;

• The Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), the Health Information Technology for Economic and Clinical Health Act (“HITECH”), Texas privacy law and other relevant legal requirements;

• Emerging regulatory compliance issues;

• Training on specific risk areas such as uses and disclosures of PHI, use of HIPAA authorizations, business associate agreements, fundraising, marketing, research, preventing and reporting breaches, and in response to specific events;

• Use of the Compliance Hotline;

• Implication of the Institutional Compliance Program and the Privacy Compliance Plan, on job requirements and as part of the employee’s annual evaluation;

• Duty to report, and consequences of the failure to report, potential violations by another employee, supervisor or outside contractor; 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. In addition, MD Anderson’s Notice of Privacy Practices, which states the Institution’s overall policies and procedures regarding privacy, is available online and in prominent areas of the Institution. Ongoing education is provided as appropriate to review privacy issues and to inform employees on new and emerging privacy information. 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 CCO, or designee, shall meet periodically with designated departmental representatives to stay abreast of current and/or new matters related to privacy compliance.

1.2 The CCO, or designees, shall monitor the progress of risk management plans.

2.0 Auditing Activities

The CCO, or designee, shall perform periodic audits or similar assurance activities regarding privacy compliance. Audits commonly performed by the CCO, or designee, include physical safeguard audits and audits of medical record access.

**CORRECTIVE AND/OR DISCIPLINARY ACTION**

MD Anderson upholds a “zero tolerance” policy towards any illegal activity or knowing, intentional or willing non-compliance. Any employee knowingly, willingly, and/or intentionally in violation of the federal and state laws, regulations, Regents’ Rules and Regulations and/or institutional policies is subject to disciplinary actions, up to and including termination. All actions taken will be in accordance with MD Anderson’s Hospital Compliance Plan.

**INVESTIGATION AND REMEDIATION**

The CCO, with support from legal counsel and the EICC, addresses any violation of the laws, regulations, and MD Anderson’s policies and standards applicable to governmental compliance. Whenever a compliance issue has been identified through the hotline, direct contact, a third-party, or other source, and a preliminary assessment suggests that an investigation is warranted, the CCO will initiate an investigation to determine the facts and circumstances of the potential violation. Alternatively, the CCO may accept a previously conducted investigation if such investigation was conducted with knowledge and approval of the CCO. Compliance investigations will be performed with the assistance of legal counsel, as needed, and will be reported immediately and confidentially to the EICC, as appropriate. If the CCO believes the integrity of the investigation is at stake, the appropriate employee(s) may be removed from duty until the investigation is completed. The CCO ensures that steps are taken to prevent destruction of documents or other evidence.

The CCO promptly and fully investigates all reports professionally and without prejudice. Consultations follow with the appropriate division head(s), manager, and/or employee, as appropriate. The corrective action plan to be implemented is determined after the outcome of each investigation. In determining the corrective action plan, MD Anderson does not take into consideration an employee’s or faculty member’s economic benefit to MD Anderson. All corrective action taken will be in accordance with MD Anderson’s Hospital Compliance Plan.
If the investigation indicates that disciplinary action is warranted, such action will be imposed in accordance with MD Anderson’s written standards of disciplinary action.

Any misconduct that violates civil or criminal law, or rules and regulations may be reported to the appropriate governing body after receipt of the credible evidence of misconduct, along with a description of the appropriate disciplinary action taken.

In the event that a privacy investigation results in the determination that a breach of PHI or breach of system security has occurred, the CCO will notify the affected individuals, government agencies, and/or media, in accordance with applicable state or federal law, within the requisite time period.

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

SANCTIONED INDIVIDUALS

MD Anderson prohibits the employment of or contracting with individuals or entities who: (a) have a criminal history related to health care; or (b) have been disbarred, excluded, or otherwise determined ineligible for participation by certain federal or state 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 person knows or should have known of, may subject a person to disciplinary action up to and including termination. MD Anderson will not accept an employee’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 CCO and the EICC, Workforce Members contacting the Institutional Compliance Office are assured non-retaliation in accordance with the Non-Retaliation Policy (UTMDACC Institutional Policy # ADM0254) and an atmosphere of confidentiality.

To report compliance concerns, Workforce Members may:

- Call the Compliance Hotline at: 1-800-789-4448;
- Contact the Institutional Compliance Office directly at: 713-745-6636; or
- Contact the CCO via the Page Operator: 713-792-7090.
- Report suspected fraud, waste, and abuse involving state resources 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, http://sao.fraud.state.tx.us.

MD Anderson has established the Compliance Hotline, listed above, for Workforce Members to report all suspected violations or questionable conduct. The hotline includes the following features:

- The 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 displayed in poster form on MD Anderson bulletin boards;
- Telephone calls to the 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 his/her name;
• Information provided to the hotline is treated as privileged to the extent permitted by applicable law;
• The CCO strictly complies with and enforces MD Anderson’s Non-Retaliation Policy (UTMDACC Institutional Policy # ADM0254).

Intentionally making false accusations is a serious violation of MD Anderson policy and will lead to disciplinary actions against the person making the accusation, up to and including termination of employment;

Employees may not use the hotline to protect themselves from the outcome of their own violations or misconduct, nor will the discipline be increased or decreased for an employee who reported his or her own violation;

Upon receiving information from the hotline, the CCO 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 CCO, 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 CCO will provide routine reports and periodic updates as deemed necessary to the EICC and President.
REFERENCES

Terms not defined in the Privacy Compliance Plan are contained in MD Anderson’s HIPAA Definition Plan.

[http://sao.fraud.state.tx.us](http://sao.fraud.state.tx.us)

**Standards of Conduct**.

**Hospital Compliance Plan**.

**Corrective Action Policy (UTMDACC Institutional Policy # ADM0256)** and Privacy Violations: Guidelines for the Application of Disciplinary Actions (Attachment # ATT1778).

**Non-Retaliation Policy (UTMDACC Institutional Policy # ADM0254)**.

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

**Policies and Procedures Related to HIPAA and Privacy**.
APPROVALS

<table>
<thead>
<tr>
<th>Date</th>
<th>Approver</th>
</tr>
</thead>
<tbody>
<tr>
<td>10-22-2019</td>
<td>Executive Institutional Compliance Committee</td>
</tr>
<tr>
<td>10-17-2018</td>
<td>Executive Institutional Compliance Committee</td>
</tr>
<tr>
<td>11-06-2017</td>
<td>Executive Institutional Compliance Committee</td>
</tr>
<tr>
<td>10-27-2016</td>
<td>Executive Institutional Compliance Committee</td>
</tr>
<tr>
<td>11-20-2014</td>
<td>Executive Institutional Compliance Committee</td>
</tr>
<tr>
<td>09-11-2013</td>
<td>Executive Institutional Compliance Committee</td>
</tr>
<tr>
<td>10-09-2012</td>
<td>Executive Institutional Compliance Committee</td>
</tr>
<tr>
<td>09-07-2011</td>
<td>Executive Institutional Compliance Committee</td>
</tr>
<tr>
<td>04-07-2010</td>
<td>Executive Institutional Compliance Committee</td>
</tr>
</tbody>
</table>

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