

**Institutional Handbook of Operating Procedures**

**Policy 6.0.1**

Section: Compliance Policies	Responsible Vice President: Senior Vice President & General Counsel
Subject: Privacy Related	Responsible Entity: Office of Institutional Compliance

**I. Title**

*Privacy Compliance Plan*

**II. Policy**

The University of Texas Medical Branch is committed to conducting its business in an ethical and law-abiding fashion. We are intolerant of fraud, abuse, waste, or other violations of any applicable federal, state, or local laws, and regulations. We will maintain a business culture that builds and promotes compliance consciousness and encourages employees and faculty to conduct all University business with honesty and integrity. Our commitment to compliance includes: communicating to all employees, faculty, consultants, and independent contractors clear business ethical guidelines to follow; providing general and specific training and education regarding applicable laws, regulations, and policies; and providing monitoring and oversight to help ensure that we meet our compliance commitment. We promote open and free communication regarding our ethical and compliance standards and provide a work environment free of retaliation.

Responsibility and accountability for actual compliance with laws, regulations, and policies rests with each individual employee. The department chairman/head or leader of each operating unit is accountable for ensuring that their subordinates are adequately trained and for detecting noncompliance with applicable policies and legal requirements when reasonable management efforts would have led to the discovery of problems or violations.

To promote compliance and implement an institutional compliance program we have developed an Office of Institutional Compliance (OIC). The OIC is responsible for developing an institutional compliance program that will promote compliance with all applicable legal requirements, foster and help ensure ethical conduct, and provide education, training, and guidance to all employees and faculty. Our institutional compliance plan and program is designed to prevent accidental or intentional noncompliance with applicable laws and regulations; to detect such noncompliance, if it occurs; to discipline those involved in noncompliant behavior, and to prevent future noncompliance.

Our compliance program has been developed to include the seven requirements of an effective compliance program included in the Federal Sentencing Guidelines.<sup>1</sup> These requirements are:

1. Establish compliance standards and procedures to be followed by employees and faculty that are reasonably capable of reducing the prospect of criminal conduct;
2. Assign high-level personnel of the organization to have overall responsibility to oversee compliance with such standards and procedures;

---

<sup>1</sup> Commentary. U. S. Sentencing Guidelines § 8A1.2.

## IHOP Policy 6.0.1 Privacy Compliance Plan

3. Use “due care not to delegate substantial discretionary authority to individuals who the organization knew, or should have known through the exercise of due diligence, had a propensity to engage in illegal activity;”
4. Communicate effectively compliance standards and procedures to all employees by requiring participation in training programs or by disseminating publications that explain in a practical manner what is required;
5. Take reasonable steps to achieve compliance with standards by utilizing monitoring and auditing systems reasonably designed to detect criminal conduct and by having in place and publicizing a reporting system whereby employees and other agents can report criminal conduct by others within the organization without fear of retribution;
6. Consistently enforce standards through appropriate disciplinary mechanisms, including discipline of individuals responsible for the failure to detect an offense; and
7. Take all reasonable steps to respond appropriately to detected offenses and to prevent further similar offenses.

The policies and procedures contained in this program are intended to establish a framework to help ensure compliance but are not to be considered all-inclusive.

### III. Standards of Conduct Guide

The University of Texas Medical Branch is committed to conducting UTMB business with integrity and in compliance with applicable laws. UTMB has developed a [\*Standards of Conduct Guide\*](#). The purpose of the *Standards of Conduct Guide* is to communicate to all UTMB employees and students an expectation and requirement of ethical conduct and compliance with applicable laws, policies, rules, and regulations. The *UTMB Standards of Conduct Guide* is a framework within which all employees are expected to operate. The *UTMB Standards of Conduct Guide* represents policies of UTMB, the University of Texas System and the *Rules and Regulations of the Board of Regents of the University of Texas System*, known as *Regents’ Rules and Regulations*. This booklet does not include all general compliance issues, nor does it contain the special compliance issues that are job specific. Instead, the *UTMB Standards of Conduct Guide* should be regarded as a set of guiding principles that apply to every UTMB employee.

The *UTMB Standards of Conduct Guide* applies to all UTMB employees, including administration, faculty, fellows, residents, and students. Moreover, the *Standards of Conduct Guide* is applicable to physicians not employed by UTMB but serving on UTMB Hospitals medical staff as well as university and hospital subcontractors, independent contractors, and consultants.

### IV. Compliance Organization and Oversight

Responsibility for oversight and implementation of the Privacy Compliance Plan rests with a multidisciplinary Information Security and Privacy Compliance Committee (ISPCC), whose membership is appointed by the Executive Institutional Compliance Committee (Executive ICC). Minutes of all meetings are maintained in a confidential manner and are provided to the Executive ICC on a quarterly basis. Minutes are maintained in the OIC.

The responsibility for implementing and managing the Institutional Compliance Program and Privacy Compliance Plan is assigned to the Chief Compliance Officer (CCO), who functions with UTMB’s organizational structure. The CCO is authorized to report to the UTMB President or the Chancellor of the UT System at any time. The CCO will with the assistance of the committee, perform the following activities:

1. Prepare and submit to the Executive ICC an annual work plan that outlines the major activities and initiatives of the ISPCC for the upcoming fiscal year;

## IHOP Policy 6.0.1 Privacy Compliance Plan

2. Prepare and submit to the Executive ICC an annual report that summarizes the ISPCC's progress regarding each work plan objective contained in the ISPCC's annual work plan for the preceding fiscal year;
3. Review the laws, regulations, statutes, policies and guidelines related to privacy;
4. Recommend the creation of new and revisions to current privacy policies and procedures;
5. Develop and implement necessary changes in practices or procedures that assure adherence to established privacy policies;
6. Develop and implement an educational training program to ensure the understanding of federal and state laws and regulations impacting privacy;
7. Conduct and coordinate investigations of alleged privacy violations;
8. Develop appropriate corrective action plans to address privacy compliance issues;
9. Handle inquiries by employees and patients regarding any aspect of privacy, and overseeing the process of uniform discipline;
10. Communicate regularly with the Executive ICC on new and emerging issues; and
11. Notify patients whose unsecured protected health information (PHI) is breached.

The CCO is designated as accountable for the day-to-day implementation of the Privacy Compliance Plan. In addition, there may be other departments throughout the institution that may have operational obligations under the Privacy Compliance Plan as determined by the CCO.

### V. Privacy Compliance Plan and Policies

The goal of the UTMB Privacy Compliance Plan is to provide guidelines that promote understanding and compliance with applicable laws, rules, and regulations, including the Health Insurance Portability and Accountability Act (HIPAA) and Family Educational Rights and Privacy Act (FERPA) and other applicable privacy regulations.

The objectives of UTMB's Privacy Compliance Plan are to:

1. Support UTMB in fulfilling its [mission](#);
2. Ensure that UTMB faculty, house staff, employees, and students understand how to appropriately handle and safeguard PHI and other sensitive personal information as well as the core responsibilities for complying with HIPAA, FERPA and other privacy and security regulations;
3. Ensure that the business of UTMB is conducted in accordance with applicable laws and regulations relating to information privacy and security;
4. Assist in identifying PHI and other personally identifiable information and the manner in which it is to be used and disclosed;
5. Establish compliance standards and procedures for UTMB Workforce Members using or otherwise coming into contact with PHI and other personally identifiable information;
6. Communicate effectively the compliance standards, policies and procedures set forth in this Privacy Compliance Plan to UTMB's Workforce Members;
7. Take reasonable steps to achieve compliance with the standards, policies and procedures set for in this Privacy Compliance Plan by, for example, implementing, monitoring and auditing systems reasonably designed to detect the improper use and disclosure of PHI; and
8. Respond appropriately to non-compliance after detection and to prevent recurrence, which may require modifications to this Privacy Compliance Plan.

### VI. Information, Education and Training

**Information-** Occasional letters, articles in Impact, the institutional semimonthly newsletter, and other publications, regarding the institutional compliance program and the OIC are sent to all employees. E-mail notifications and communications are also sent to employees. The content of these publications

## IHOP Policy 6.0.1 Privacy Compliance Plan

may be related to specific, and or general compliance issues and other elements of the program. Every employee is provided access to the UTMB Standards of Conduct Guide and is required to acknowledge annually that they will abide by UTMB's Standards of Conduct. Additionally, all employees are expected to read the Privacy Compliance Plan and understand its principles. Given the complexity of privacy regulations impacting UTMB, employees may need further clarification beyond the materials contained in this plan. All employees with questions regarding the Privacy Compliance Plan or privacy requirements in general are encouraged to seek answers and/or clarification from the OIC in accordance with Reporting Privacy Concerns and Questions in this document.

***Education and Training-*** UTMB is committed to communicating our standards for ethical conduct and UTMB policies to all employees. The OIC provides education and training to develop compliance awareness and commitment. All administration, faculty, medical staff, and employees must complete general compliance training in accordance with UTMB's Institutional Compliance Plan.

Compliance with all applicable government regulations is one of UTMB's most important priorities. All members of the UTMB workforce must be knowledgeable about UTMB's Institutional Compliance Program and the Privacy Compliance Plan. Education and training programs related to the Privacy Compliance Plan include such topics as:

1. General privacy compliance and best practices for HIPAA, FERPA, Texas privacy law and other relevant legal requirements;
2. Uses and/or disclosures of PHI, and the required patient and/or statutory permissions for each purpose;
3. Newly adopted, revised and established UTMB policies and procedures regarding privacy;
4. Implications of failing to adhere to the Privacy Compliance Plan and all applicable program requirements;
5. Training on specific risk areas such as uses and disclosures of PHI, business associates, marketing and research;
6. Use of the Fraud, Abuse and Privacy Hotline;
7. Duty to report, and consequences of the failure to report, potential violations by another employee, supervisor or outside contractor; and
8. Identity theft prevention, detection, and mitigation

A variety of teaching materials, tools, and methods are used as necessary. Ongoing education is provided as appropriate to review privacy issues and to inform employees on new and emerging privacy information.

### **VII. Maintenance of Training Documentation and Disciplinary Action**

Compliance training is required of all employees and is considered a condition of employment. Failure to meet education and training requirements will result in disciplinary action, up to and including termination. All persons in supervisory positions are responsible for ensuring that each UTMB employee reporting to them has completed the compliance training applicable to that person. Completion of required compliance training will be closely monitored and documented. The UTMB Human Resources Department maintains training records and reports detailed training activities for employees. Summary reports of compliance with education and training requirements are provided to the Executive ICC.

## IHOP Policy 6.0.1 Privacy Compliance Plan

### VIII. Adherence to the Compliance Program as a Requirement for Promotion for Faculty and as an Element for Evaluating all Employees

#### Faculty

Adherence to the UTMB institutional compliance program is a part of each faculty member's annual evaluation and is also used as a criterion for promotion in academic rank. It is understood that the Appointment Promotion and Tenure Committee of each UTMB school should consider participation in compliance training and any involvement in compliance infractions as a part of the promotion evaluation process.

#### Managers and Supervisors

Managers and supervisors include all individuals who have as part of their job descriptions the supervision of any UTMB employee. The promotion of and adherence to the institutional compliance program by all management and supervisors is considered an integral part of their job performance. At UTMB, employees' awareness of and adherence to the institutional compliance program should be used as an element or measurement tool in the evaluation process for continuing employment and promotions.

- **Education and Training**

Managers and supervisors are required to ensure and verify that employees complete all mandatory and elective training assigned to the employee including compliance training at UTMB. Managers and supervisors should inform employees that UTMB will take disciplinary action for violation of policies, procedures, and regulatory requirements, or for failure to complete mandatory training requirements. Moreover, employees are informed that strict adherence to the laws, regulations, and policies are a condition of employment.

- **Inform Employees**

Managers and supervisors are responsible for informing employees of compliance policies and procedures specifically related to their job function and appropriately monitoring employees to help ensure adherence to policies and procedures.

### IX. Risk Assessment and Work Plan

#### Risk Assessment Profile

The UTMB OIC assesses institutional risk on an ongoing basis as a matter of conducting daily activities for purposes of:

- Identifying high-risk compliance issues;
- Establishing a priority for these issues;
- Establishing monitoring activities designed to review processes and strengthen compliance; and
- Preparing the OIC annual work plan.

#### Work Plan

In conjunction with the Executive ICC the OIC will create an annual work plan to review high risk items identified through the risk assessment process. The work plan will also include other items and/or issues in which the OIC expects to be involved in during that fiscal year.

### X. Compliance Monitoring

In order to ensure successful implementation of the Privacy Compliance Plan and compliance with applicable federal, state, and local regulations, the CCO, with support of the ISPPCC, conducts periodic audits of operations. The audits are designed to specifically identify areas deemed to be privacy risks, as

## IHOP Policy 6.0.1 Privacy Compliance Plan

well as randomly selected processes, where corrective action may be required. At a minimum, these audits address the following areas:

1. Uses and disclosures of PHI;
2. Marketing and fundraising practices;
3. Notice of Privacy Practices acknowledgements;
4. Administration of patients' rights;
5. Contractual requirements, such as Business Associate Agreements;
6. Adherence to the minimum necessary standard; and
7. Other workforce activities directly related to privacy practices.

Audits include:

- a. On-site visits;
- b. Interviews with personnel involved in administration, operations, billing, marketing, and other related activities;
- c. Review of policies, procedures, and written documentation used by members of the UTMB workforce; and
- d. Trend analysis studies.

The OIC will facilitate subsequent audits or studies to ensure the successful implementation of corrective actions.

### **XI. Reporting Violations or Questionable Conduct**

#### **Employee's Responsibility**

It is every employee's responsibility to report suspected violations of laws, regulations, policies or questionable conduct. 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. UTMB has established methods for employees to report, confidentially and anonymously, any questionable conduct or possible violation(s). Individual employees may discuss concerns with their supervisor or directly with the CCO by contacting the OIC directly at: 409-747-8700. Additional methods for reporting are described below.

All employees with questions regarding the Privacy Compliance Plan or other compliance requirements in general are encouraged to seek answers and/or clarification from the OIC.

#### **Fraud, Abuse and Privacy Hotline (1-800-898-7679)**

UTMB has established a dedicated Fraud, Abuse and Privacy Hotline as an internal reporting mechanism for reporting suspected waste, abuse, fraud, or other illegal conduct of UTMB employees, students, vendors, or independent contractors. The UTMB Fraud, Abuse and Privacy hotline is available 24 hours a day, 365 days a year by calling 1 (800) 898-7679.

Individuals may also 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>.

#### **Confidential and Anonymous**

UTMB will ensure the anonymity, to the extent allowed by law, of individuals who report violations or questionable conduct. All reported allegations or concerns will be investigated confidentially.

## IHOP Policy 6.0.1 Privacy Compliance Plan

### **Intentional False Accusations**

UTMB will consider it a serious violation of UTMB policy for employees to intentionally make false accusations. Such false accusations may result in disciplinary action, up to and including termination, against the accuser. All reports to the UTMB OIC should be made in good faith and with the best of intentions.

### **Non-retaliation Policy**

Employees are encouraged to freely discuss and raise questions to managers or to any appropriate personnel about situations they may feel are in violation of applicable laws, regulations, rules, policies, and procedures. Moreover all UTMB employees have a personal obligation to report any activity that appears to violate applicable laws, regulations, rules, policies, and procedures. Employees wishing to remain anonymous may file a report via the UTMB Fraud, Abuse and Privacy Hotline (800-898-7679). UTMB shall not intimidate, threaten, coerce, discriminate against, or take any retaliatory action against any individuals who in good faith report suspected wrongdoing to their supervisor or through the UTMB Fraud, Abuse and Privacy Hotline.

## **XII. Response to Allegations, Identified Problems, and Audit Outcomes**

### **Investigation**

All reports of potential violations of laws, regulations, policies or questionable conduct, from any source, shall be logged and presented to the CCO. A report of the investigation, including findings and recommendations, will be created. The CCO will assign the Privacy Officer to investigate and/or coordinate investigations. The Privacy Officer completes a formal written report to the CCO including the nature of the suspected violation or complaint, the names of the individuals associated with the suspect behavior and data to support or refute the claims. Analysts may be brought in as resources to assist in investigations; however, they are considered fact finders and make no determinations with regard to disciplinary actions. The Privacy Office will use best efforts to complete the investigation in a prompt manner with a report and recommendations to the CCO. Investigations include interviews and a review of relevant documents. 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.

Following the investigation, the CCO may prepare a report to the IPC, describing the findings and identifying the steps and accountability structure to rectify any issues noted. The report may be presented to the Executive ICC during its quarterly monthly meeting, or at a specially convened meeting, for an official ruling, if necessary, on the incident. The CCO apprises the President as necessary.

Investigations resulting in extensive corrective action and/or disciplinary action shall be reviewed and approved by the CCO prior to implementation. The Executive ICC will be informed of these actions and following discussion may direct further action.

### **Recommendations**

#### **Corrective Action**

When an instance of non-compliance has been determined and confirmed by the CCO, a corrective action plan will be submitted to the CCO. The corrective action plan will focus on implementing changes in internal processes to improve, prevent, or detect compliance inadequacies. The CCO may notify and meet with the department Chair and/or the department management, the affected faculty member(s) or employee(s) and explain the corrective action to be implemented. The corrective action plan may include one or all of the following elements:

1. Specific areas requiring compliance attention;
2. Requirement of additional training;

## IHOP Policy 6.0.1 Privacy Compliance Plan

3. Ceasing problematic process;
4. Change in policies and procedures;
5. Repaying overpayments;
6. Reporting to the appropriate governmental authorities;
7. Further audit and/or investigation;
8. Determining whether the problem is systematic; and
9. Disciplinary action.

### **Disciplinary Action**

Disciplinary action in accordance with UTMB's written standards of disciplinary action may be imposed as a part of a corrective action plan for all UTMB administration, faculty, house staff, and employees.

### **Obligation to Report**

Reports or allegations that may constitute intentional violation or reckless disregard of criminal, civil, or administrative law shall be referred to UTMB legal authorities for investigation and disposition. If the investigation produces credible evidence that provides a reasonable basis to conclude that a violation of law may have occurred, UTMB shall promptly provide all information to the appropriate legal authorities for a determination of prosecution.

## **XIII. Disciplinary Action and Appeal**

UTMB will impose disciplinary action on employees who fail to comply with applicable laws, regulations, and policies. The seriousness of the violation will determine the level of the disciplinary action.

### **Faculty**

#### **Disciplinary Action**

##### **a) Recommendation of disciplinary action related to compliance issues**

The UTMB Executive ICC may make recommendations related to disciplinary action of faculty regarding compliance violations up to and including termination. Disciplinary action and termination will be conducted according to *Rules and Regulations of the Board of Regents of the University of Texas System*.

##### **b) Recommendation of summary dismissal**

Reports or allegations that may constitute an intentional violation or reckless disregard of criminal, civil, or administrative law shall be given to UTMB legal authorities for investigation and disposition. Notwithstanding the foregoing, following the determination that a reckless disregard or intentional violation of law has occurred, the Dean of the appropriate school of the faculty member may recommend to the President to proceed with charges for termination, depending upon the nature of the conduct. Procedures for termination shall be according to the *Rules and Regulations of the Board of Regents of the University of Texas System*.

### **Appeal**

Appeal of a UTMB disciplinary action shall be according to the appeals procedure in Section 6 of the *Rules and Regulations of the Board of Regents of the University of Texas System*. No other internal appeal process is available to a disciplined faculty other than as provided by the *Regents' Rules*.

### **Non-employee Medical Staff**



## IHOP Policy 6.0.1 Privacy Compliance Plan

### **Disciplinary Action**

Disciplinary action administered to non-employee medical staff will follow the guidelines as outlined in the UTMB Medical Staff By-laws.

### **Appeal**

Non-employee Medical Staff are subject to the appeals procedures outlined in the UTMB Hospitals Medical Staff By-laws.

### **House Staff**

#### **Disciplinary Action**

Disciplinary action administered to house staff is in accordance with the UTMB House Staff Work Agreement and the Office of the Associate Dean for Graduate Medical Education.

#### **Appeal**

Appeals for disciplinary actions administered to house staff are in accordance with the UTMB House Staff Work Agreement.

### **Classified Employees**

#### **Disciplinary Action**

Disciplinary action related to classified employees will be administered in accordance with the disciplinary action provided for in the *UTMB Institutional Handbook of Operating Procedures (IHOP) Policy 3.10.1 Discipline, Dismissal and Appeal for Classified Employees*. Any recommendations of disciplinary action shall be managed pursuant to IHOP and the *Rules and Regulations of the University of Texas Board of Regents*.

#### **Appeal**

Appeal for disciplinary action administered to classified employees is in accordance with the appeals procedure provided for in *IHOP Policy 3.10.1 Discipline, Dismissal and Appeal for Classified Employees*.

## **XIV. Responding to Inquiries**

If any member of the UTMB workforce receives an oral or written inquiry regarding UTMB's compliance with any law or regulation, from any source whether governmental or private, the employee shall immediately notify the OIC prior to responding in any way to the inquiry.

OIC staff will:

1. Identify the person or entity making the inquiry;
2. Verify the authority for the inquiry; and
3. Determine the nature of the inquiry.

## **XV. Record Creation and Retention**

The CCO ensures that all records created, maintained and safeguarded by the OIC are retained on an ongoing basis in accordance with *IHOP Policy 2.1.4 Records and Information Management and Retention*. All UTMB contracts must require that the contracted parties adhere to the Standards of Conduct and the Record Retention Policy. When the contractor is a Business Associate as defined by HIPAA, appropriate language detailing the contractor's responsibilities for using, disclosing, and maintaining PHI is also included. To assure overall compliance, the CCO is authorized, along with UTMB's legal counsel, to negotiate contracts with all third parties.

## IHOP Policy 6.0.1 Privacy Compliance Plan

UTMB has adopted the following standards to assist the CCO with oversight of all documents required by law and necessary to its operations:

1. Institutional Compliance Program investigation files shall include the following information:
  - a. alleged violation;
  - b. investigative process;
  - c. copies of interview notes;
  - d. key documents;
  - e. log of witnesses interviewed;
  - f. documents reviewed; (g) results of the investigation; and
  - g. corrective action implemented, as needed;
2. No employee may enter false or misleading information into UTMB records;
3. Records shall be organized in a manner that facilitates prompt retrieval;
4. All records shall be stored in a safe and secure manner for the period required by federal and state law or by UTMB policy, whichever is longer;
5. Records shall be destroyed when no longer needed to be retained under federal and state law or UTMB policy, whichever is longer;
6. Adequate records shall be developed and maintained to document UTMB's compliance with all applicable laws;
7. The confidentiality and security of records shall be appropriately assured and adhered to based on federal and state laws and UTMB policies; and,
8. No employee may destroy or alter any UTMB record if the CCO or appropriate designee has notice of any pending litigation or governmental investigation, litigation, claim, negotiation, audit, open records request, administrative review, or if any other action involving such record is initiated before the expiration of the retention period and subsequent destruction of such record.

### XVI. Revisions to Privacy Compliance Plan

This compliance plan is intended to be flexible and readily adaptable to changes in regulatory requirements. The ISPCC shall review the plan at least annually to assure that it remains current and effective. Changes to the plan may be proposed by members of the Executive ICC, ISPCC, departments, or individual employees. Any recommendations for changes to the plan must be approved by the ISPCC. All changes to the compliance plan must be consistent with the Institutional Handbook of Operating Procedures and the *Rules and Regulations of the Board of Regents of the University of Texas System*.

### XVII. Related UTMB Policies and Procedures

[UTMB Standards of Conduct Guide](#)

[IHOP 6.2.39 Privacy Incident Response and Breach Notification](#)

[IHOP 3.2.9 Non-Retaliation Policy](#)

[IHOP 3.1.9 Discipline, Dismissal and Appeal for Classified Employees](#)

[IHOP 6.1.5 Records and Information Management and Retention](#)

### XVIII. Dates Approved or Amended

<i>Originated:</i> 12/09/2010	
<i>Substantive Revisions</i>	<i>Non-Substantive Revisions</i>
11/30/2011	11/26/2014

### XIX. Contact Information

Office of Institutional Compliance  
(409) 747-8700

**IHOP Policy 6.0.1 Privacy Compliance Plan**