EXHIBIT "B"

THE UNIVERSITY OF TEXAS
MD Anderson Cancer Center
Making Cancer History®

MD Anderson Institutional Policy # ADM0264

Confidentiality Policy

Purpose

The purpose of this policy is to:

- Uphold the confidentiality of health information, and protect the privacy of patients, research participants, faculty, trainees/students, and other members of MD Anderson's workforce, and the institution; and
- Assure that all faculty, trainees/students, and other members of MD Anderson's workforce are aware of the limits on disclosure of Confidential Information and Sensitive Information.

Policy Statement

It is the policy of The University of Texas MD Anderson Cancer Center (MD Anderson) to protect Confidential Information and Sensitive Information to the extent permitted or required by law, including as such information relates to patients, research participants, students, and faculty, trainees and other members of MD Anderson's workforce; and institutional business matters, including as such matters pertain to pending litigation, intellectual property/scientific discoveries, and facility information.

Faculty, trainees, students, and other members of MD Anderson's workforce have an obligation to respect the privacy of all patients and hold in confidence all information gathered in the course of delivering care, or as informally observed.

All Protected Health Information is regarded as Confidential Information and made available only to authorized individuals or as required by law.

Education records may be used by or disclosed to individuals as permitted by the Family Educational Rights and Privacy Act of 1974 and 34 CFR Part 99 (FERPA).

Employee data is to be used only in the completion of official duties and disclosed only to those persons with a business need-to-know or under legal requirements.

Appropriate safeguards will be maintained to protect against inappropriate access, destruction or disclosure of paper and electronic information.

> *Note:* This policy is intended to serve as a roadmap to MD Anderson's collection of privacy policies. For detailed privacy guidance governing the matters herein, see the MD Anderson institutional policies referenced within the body of this policy and listed in the Reference Section below.

Scope

This policy applies to all faculty, trainees/students, and other members of MD Anderson's workforce, clinical trial monitors, visiting scientists, as well as other visitors accompanying faculty members, vendors, and consultants. This policy also applies to information in all forms (*e.g.*, oral or written - whether hard copy or electronic).

Compliance with this policy is the responsibility of all faculty, trainees/students, and other members of MD Anderson's workforce.

Target Audience

The target audience for this policy includes, but is not limited to, all faculty, trainees/students, and other members of MD Anderson's workforce.

Definitions

Confidential Information: Information including, but not limited to:

- Health information relating to patients, research participants, and/or faculty, trainees/students, and other members of MD Anderson's workforce, including, but not limited to, records containing Protected Health Information (PHI);
- Education Records, as defined by FERPA;
- Financial information, including, but not limited to, account numbers;
- Personnel and security information, including, but not limited to, Social Security numbers, driver's license numbers, or other government-issued identification numbers;
- Proprietary information related to research, intellectual property, and/or scientific discoveries;
- All business and litigation information not deemed a Matter of Public Record; and/or
- Any other information considered confidential by law.

See also MD Anderson's **Data Classification Guidelines and Ratings**.

Electronic Health Record (EHR) System: An integrated system of applications that work together to support patient care processes by integrating data from multiple sources, capturing data at the point of care, supporting caregiver decision-making, enabling appropriate documentation of and reimbursement for the care provided, and facilitating the dissemination of that data with patients, referring providers, and other entities with a clinical, research, or business reason to access patient information.

Health Care Operations: See **HIPAA Definitions Plan**.

HIPAA: Health Insurance Portability and Accountability Act of 1996.

Matter(s) of Public Record: Event(s) about which information has been deemed available to the public (*e.g.*, traffic and industrial accidents, crimes, and deaths).

Payment: See **HIPAA Definitions Plan**.

Protected Health Information (PHI): See **HIPAA Definitions Plan**.

Sensitive Information: Information maintained by the institution that, while not Confidential Information, requires special precautions in order to prevent any disclosure that might harm or embarrass the subject of such information, including a patient, research participant, and/or faculty member, trainee/student, or other member of MD Anderson's workforce, or the institution.

Treatment: See **HIPAA Definitions Plan**.

Procedure

1.0 Confidentiality of Patient Information

1.1 Protected Health Information (PHI):

A. Information concerning MD Anderson patients is confidential and protected by federal and state law.

B. Unless one of the exceptions outlined in MD Anderson's **Patient Privacy: Authorization for the Use and Disclosure of Protected Health Information Policy (UTMDACC Institutional Policy # ADM0396)** applies (*e.g.*, Treatment, Payment, Health Care Operations, or other disclosures authorized by law), an individual's PHI may not be used or disclosed without first obtaining the individual's written HIPAA authorization. See also **Patient Privacy: Uses and Disclosures of Protected Health Information Policy (UTMDACC Institutional Policy # ADM0401)**.

C. The privacy and confidentiality of the patient must be respected at all times, including during:

- Case discussions, which are confidential and should not be conducted within the hearing of non-participants, and
- Examinations and Treatment, which should be conducted as discreetly as possible.

D. Disposal of PHI should be performed in accordance with applicable legal and regulatory requirements, and through established institutional procedures designed to protect patients, faculty, trainees/students, and other members of MD Anderson's workforce, and the institution. Paper documents containing Confidential Information and/or Sensitive Information (including PHI) that need to be disposed of must be shredded or placed in institutional secured shredding bins. PHI maintained in electronic form must be disposed of in accordance with secure methods of sanitation or destruction approved by the U.S. Department of Health and Human Services. See: MD Anderson's **Disposal of Confidential and/or Sensitive Information Policy (UTMDACC Institutional Policy # ADM0389)** and **Information Resources Security Operations Manual**.

1.2 Patient Rights:

A. Notice of Privacy Practices:

Patients have the right to receive a copy of MD Anderson's Joint Notice of Privacy Practices at any time upon request. MD Anderson provides patients with its Joint Notice of Privacy Practices at or before new patient registration and makes available an electronic copy of its **Joint Notice of Privacy Practices** on its internet page. See: MD Anderson's **Patient Privacy: Joint Notice of Privacy Practices Policy (UTMDACC Institutional Policy # ADM0395)**.

B. Right to Accounting of Disclosures:

Patients have the right to receive an accounting, or list, of certain disclosures made by MD Anderson of their PHI, including disclosures made to or by MD Anderson's business associates. See: MD Anderson's **Patient Privacy: Right to Receive Accounting of Disclosures Policy (UTMDACC Institutional Policy # ADM0392)**.

C. Right to Request Amendment of PHI:

Patients have the right to request amendment of their PHI maintained in the designated record set for as long as the information is kept by or for MD Anderson. See MD Anderson's **Patient Privacy: Right to Request Amendment of PHI Policy (UTMDACC Institutional Policy # ADM0390)**.

D. Right to Inspect and Copy PHI:

Patients have a right of access to inspect and obtain a copy of their PHI maintained in the designated record set. See MD Anderson's **Patient Privacy: Right to Access Protected Health Information Policy (UTMDACC Institutional Policy # ADM0391)**.

E. Right to Request Alternate Communication Methods or Locations:

Patients have the right to request that MD Anderson communicate with them about medical matters in a certain way or at a certain location (*e.g.*, a patient may ask that MD Anderson only contact him/her by telephone at work or by mail at home or an alternative address). MD Anderson will attempt to accommodate all reasonable requests. MD Anderson may condition approval, when appropriate, upon receiving information as to how payment, if any, for the patient's care will be handled. Note: MD Anderson requires that all such requests: (1) be in writing; (2) be directed to the Chief Privacy Officer for approval; and (3) specify how or where the patient wishes to be contacted. See: MD Anderson's **Patient Privacy: Right to Request Restrictions Policy (UTMDACC Institutional Policy # ADM0393)**.

F. Right to Request Restrictions:

Patients may make a written request to restrict the use and/or disclosure of their PHI (*e.g.*, a request that medical records not be released through electronic health information exchanges, or requests for the protections provided under the "confidential patient type" in the Electronic Health Record System). It is the policy of MD Anderson to accommodate reasonable restriction requests (*e.g.*, to the extent to which it does not impede patient care or conflict with other business, regulatory or legal requirements). A request for a restriction must be made in writing. See MD Anderson's **Patient Privacy: Right to Request Restrictions Policy (UTMDACC Institutional Policy # ADM0393)**.

1.3 Use and Disclosure of PHI:

A. While providing care to patients, faculty, trainees/students, and other members of MD Anderson's workforce may have access to a patient's PHI. Such information is Confidential Information and should be discussed only with those persons having a professional need-to-know. Except for Treatment purposes, discussions about the patient and printed medical information should be limited to the minimum amount of information necessary to accomplish the intended purpose. See: MD Anderson's **Patient Privacy: Uses and Disclosures of Protected Health Information Policy (UTMDACC Institutional Policy # ADM0401)**.

B. Sharing PHI with individuals not involved in the patient's care is not permitted unless authorized by the patient or the patient's legally authorized representative, or in the case of a minor, the patient's parent or legal guardian. This includes identifying a person being treated at MD Anderson in a conversation with a member of MD Anderson's workforce who is not involved in the patient's care, a friend, a family member, or any other outsider. See: MD Anderson's **Patient Privacy: Disclosures of a Patient's Protected Health Information to Individuals Involved in the Patient's Care Policy (UTMDACC Institutional Policy # ADM1032)**.

C. Paper documents containing PHI must be protected and handled in accordance with state and federal laws governing the protection and confidentiality of PHI. See: MD Anderson's **Patient Privacy: Safeguarding Paper PHI Policy (UTMDACC Policy # ADM1176)**.

D. Electronic documents containing PHI must be protected and handled in accordance with state and federal laws governing the protection and confidentiality of PHI. See: MD Anderson's **Information Security Office Policy for the Use and Protection of Information Resources (UTMDACC Institutional Policy # ADM0335)** and the **Information Resources Security Operations Manual** and **Electronic Confidential and Restricted Confidential Information Access and Storage Policy (UTMDACC Institutional Policy # ADM1187)**.

E. Faculty, trainees/students, and other members of MD Anderson's workforce should contact the Director for Health Information Management (HIM) or his/her designee, if there is any doubt regarding whether or not a release of PHI is acceptable. The HIM Director or his/her designee may seek advice from the Legal Services Department or the Institutional Compliance Office (ICO). See: MD Anderson's **Official Medical Record Policy (UTMDACC Institutional Policy # CLN0554)**.

F. In the event of a known or a suspected unauthorized disclosure of PHI, faculty, trainees/students, and other members of MD Anderson's workforce must contact the ICO at 713-745-6636 or call the Privacy Hotline at 1-888-337-7497. The ICO will investigate the incident in accordance with institutional policy and the ICO's departmental procedures. See: MD Anderson's **Patient Privacy: Breach Notification Policy (UTMDACC Institutional Policy # ADM1033)**.

1.4 Death Announcements:

A. MD Anderson may disclose PHI for the purpose of death certification. Patient deaths reported to the Bureau of Vital Statistics are Matters of Public Record. See MD Anderson's **Care of the Deceased Policy (UTMDACC Institutional Policy # CLN1084)**.

B. Before External Communications announces or confirms a patient's death publicly or to the media, it will verify through the attending physician that the patient's next-of-kin has been notified of the death. External Communications should be the single source for all news media inquiries. See: MD Anderson's **News Media Assistance Policy (UTMDACC Institutional Policy # ADM0414)**.

1.5 Marketing, Advertising, and Fundraising:

A. Use and disclosure of PHI for marketing and advertising purposes is governed by MD Anderson's **Patient Privacy: Marketing Policy (UTMDACC Institutional Policy # ADM0353)** and **Advertising Placement Policy (UTMDACC Policy # ADM0351),**

B. Use and disclosure of PHI for fundraising purposes is governed by MD Anderson's **Patient Privacy: Fundraising Policy (UTMDACC Institutional Policy # ADM0162)**.

1.6 Patient Advocacy Information:

All Patient Advocacy information is Confidential Information. See: MD Anderson's **Confidentiality of Patient Advocacy Information Policy (UTMDACC Institutional Policy # ADM0350).**

2.0 Social Security Numbers:

2.1 Faculty, trainees/students, and other members of MD Anderson's workforce are prohibited from requiring an individual to disclose his/her Social Security number unless the institution is legally required to collect the Social Security number. In addition, all members of MD Anderson's workforce are prohibited from disclosing Social Security numbers to unauthorized persons or entities. See: MD Anderson's **Protecting the Confidentiality of Social Security Numbers Policy (UTMDACC Institutional Policy # ADM0159)**.

2.2 Each time a faculty member, trainee/student, or other member of MD Anderson's workforce initially requests that an individual disclose his/her Social Security number, the member of MD Anderson's

workforce must provide the individual with notice that is required under MD Anderson's **Protecting the Confidentiality of Social Security Numbers Policy (UTMDACC Institutional Policy # ADM0159)**.

3.0 Confidentiality of Employee Information

3.1 The release of Confidential Information regarding employees must be approved through the Public Information Act governance process or by the Human Resources Operations Department. See: MD Anderson's **Release of Employee Information Policy (UTMDACC Institutional Policy # ADM0281)**.

3.2 In the course of their duties, faculty, trainees/students, and other members of MD Anderson's workforce may have possession or access to Confidential Information or Sensitive Information about other members of MD Anderson's workforce (*e.g.*, salaries, personal data, medical reports, performance evaluations, planned job changes). Such information should be disclosed only to other individuals who have a business need-to-know. Caution should be exercised when handling such information in order to protect confidentiality (*e.g.*, do not leave exposed information openly exposed on your desk or computer screen; use confidential envelopes).

3.3 Confidential Information or Sensitive Information regarding faculty, trainees/students, and other members of MD Anderson's workforce may be removed from MD Anderson facilities only as required for official duties. All such material or reproductions must be immediately returned when the task requiring removal from MD Anderson is completed or upon termination of employment.

3.4 Employees who are also MD Anderson patients will be assigned the "Employee" patient type. This patient type triggers a "break the glass" screen to appear to the user on a periodic basis. The "break the glass" screen informs the user that the record is restricted, and prompts the user to document the user's reason for accessing the record.

4.0 Confidentiality of Student Information

FERPA protects the privacy of Education Records and Personally Identifiable Information contained in Education Records, as those terms are defined by 34 C.F.R. § 99.3. FERPA also gives students certain rights with respect to their Education Records. MD Anderson will use and/or disclose Education Records in accordance with FERPA and other applicable state and federal laws.

5.0 Confidentiality of Institutional Information

5.1 In addition to patient information and information about faculty, trainees/students, and other members of MD Anderson's workforce, Confidential Information includes, but is not limited to, financial data, intellectual property, research data, information related to MD Anderson's facilities (including files or documents that describe or identify the building or room name, location, type, purpose, or any negotiated contract pricing in any format) and information technology documentation. Unauthorized disclosure of this Confidential Information may have a significant adverse impact on the institution. Therefore, individuals must take all necessary precautions to protect the privacy and confidentiality of institutional Confidential Information.

5.2 The Board of Regents of the UT System owns the following types of intellectual property:

A. Intellectual property created by an individual within the course of his/her employment responsibility to MD Anderson, The University of Texas (UT) System, or any of its member institutions; and

B. Intellectual property resulting from activities performed on MD Anderson time, with the support of State funds, or from using the resources and facilities owned by MD Anderson.

5.3 Intellectual property should be disclosed to MD Anderson's Office of Technology Commercialization as soon as conceived and/or reduced to practice (and in all events prior to public disclosure). Public disclosure of intellectual property should not occur until authorized by MD Anderson. See: MD Anderson's **Intellectual Property Policy (UTMDACC Institutional Policy # ADM0345)**.

5.4 The transmittal of Confidential Information and proprietary information should contain a statement limiting unauthorized review, disclosure, use, dissemination, distribution, or copying. See: MD Anderson's **Confidentiality and/or Proprietary Information Statement Policy (UTMDACC Institutional Policy # ADM0936)**.

6.0 Miscellaneous

6.1 News Media:

A. The Communications Office is responsible for coordinating release of all information to news media. For urgent media needs after hours and on weekends and holidays, faculty, trainees/students, and other members of MD Anderson's workforce may contact the On-Call Administrator who will contact a representative of the Communications Office staff at home through the switchboard operator. See: MD Anderson's **News Media Assistance Policy (UTMDACC Institutional Policy # ADM0414)**.

B. Any release of information to the news media regarding a patient or visitor who is a public figure will be handled by the Communications Office. See: MD Anderson's **Patient Privacy: Public Figures Policy (UTMDACC Institutional Policy # ADM1179)**.

6.2 Information Resources:

A. Access to information resources by faculty, trainees/students, and other members of MD Anderson's workforce requires a unique user identification and password. Log-on IDs, passwords, telephone calling cards and other means of access must not be shared with anyone. Members of MD Anderson's workforce are responsible for assuring that electronic confidential information is stored in accordance with the **Electronic Confidential and Restricted Confidential Information Access and Storage Policy (UTMDACC Institutional Policy # ADM1187)**. Individuals are responsible for unauthorized access to information resources that result from their negligence in maintaining the confidentiality of their identification. See: MD Anderson's **Information Security Office Policy for the Use and Protection of Information Resources (UTMDACC Institutional Policy # ADM0335)**.

B. Use of personally owned mobile devices to conduct business on behalf of MD Anderson, including using such devices to access institutional information, is governed by MD Anderson's **Use of Personally-Owned Mobile Devices for Institutional Business Policy (UTMDACC Institutional Policy # ADM1188)**.

C. Electronic information access is governed by MD Anderson's **Electronic Confidential and Restricted Confidential Information Access and Storage Policy (UTMDACC Institutional Policy # ADM1187),** the **Information Security Office Policy for the Use and Protection of Information Resources (UTMDACC Institutional Policy # ADM0335)**, and the "Procedure for Accessing Employee-Stored Information" in the **Use of Information Technology Policy (UTMDACC Institutional Policy # ADM0263)**.

6.3 Public Information Act:

A. The Texas Government Code gives the public the right to access certain government records. As a State agency, MD Anderson must promptly release most requested information that is not confidential by law, either constitutional, statutory, or by judicial decision.

B. For purposes of responding to requests under the Texas Public Information Act (PIA), the Vice President and Chief Financial Officer is designated as MD Anderson's Public Information Officer

EXHIBIT "B"

(PIO). PIA requests for must be referred to the PIO immediately. The PIO will establish reasonable procedures for inspecting or copying public information and inform requestors of these procedures. There may be charges for providing the requested information, particularly if copies are provided. The PIO will coordinate the release of the requested information. See: MD Anderson's **Public Information Act** internet page for more information.

6.4 Policy Violations:

Violation of this policy may result in disciplinary action in accordance with MD Anderson's **Disciplinary Action Policy (UTMDACC Institutional Policy # ADM0256)** up to and including termination of employment.

Attachments/Links

Data Classification Guidelines and Ratings.

HIPAA Definitions Plan (Attachment # ATT0699).

Information Resources Security Operations Manual.

Joint Notice of Privacy Practices.

Public Information Act.

Related Policies

Advertising Placement Policy (UTMDACC Policy # ADM0351).

Care of the Deceased Policy (UTMDACC Institutional Policy # CLN1084).

Confidentiality and/or Proprietary Information Statement Policy (UTMDACC Institutional Policy # ADM0396).

Confidentiality of Patient Advocacy Information Policy (UTMDACC Institutional Policy # ADM0350).

Disciplinary Action Policy (UTMDACC Institutional Policy # ADM0256).

Disposal of Confidential and/or Sensitive Information Policy (UTMDACC Institutional Policy # ADM0389).

Electronic Confidential and Restricted Confidential Information Access and Storage Policy (UTMDACC Institutional Policy # ADM1187).

Information Security Office Policy for the Use and Protection of Information Resources (UTMDACC Institutional Policy # ADM0335).

Intellectual Property Policy (UTMDACC Institutional Policy # ADM0345).

News Media Assistance Policy (UTMDACC Institutional Policy # ADM0414).

Official Medical Record Policy (UTMDACC Institutional Policy # CLN0554).

Patient Privacy: Authorization for the Use and Disclosure of Protected Health Information Policy (UTMDACC Institutional Policy # ADM0396).

Patient Privacy: Breach Notification Policy (UTMDACC Institutional Policy # ADM1033).

Patient Privacy: Disclosures of a Patient's Protected Health Information to Individuals Involved in the Patient's Care Policy (UTMDACC Institutional Policy # ADM1032).

Patient Privacy: Fundraising Policy (UTMDACC Institutional Policy # ADM0162).

Patient Privacy: Joint Notice of Privacy Practices Policy (UTMDACC Institutional Policy # ADM0395).

Patient Privacy: Marketing Policy (UTMDACC Institutional Policy # ADM0353).

Patient Privacy: Public Figures Policy (UTMDACC Institutional Policy # ADM1179).

EXHIBIT "B"

Patient Privacy: Right to Access Protected Health Information Policy (UTMDACC Institutional Policy # ADM0391).

Patient Privacy: Right to Receive Accounting of Disclosures Policy (UTMDACC Policy # ADM0392).

Patient Privacy: Right to Request Amendment of PHI Policy (UTMDACC Institutional Policy # ADM0390).

Patient Privacy: Right to Request Restrictions Policy (UTMDACC Institutional Policy # ADM0393).

Patient Privacy: Safeguarding Paper PHI Policy (UTMDACC Policy # ADM1176).

Patient Privacy: Uses and Disclosures of Protected Health Information Policy (UTMDACC Institutional Policy # ADM0401).

Protecting the Confidentiality of Social Security Numbers Policy (UTMDACC Institutional Policy # ADM0159).

Release of Employee Information Policy (UTMDACC Institutional Policy # ADM0281).

Use of Information Technology Policy (UTMDACC Institutional Policy # ADM0263).

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

Joint Commission Standards / National Patient Safety Goals

IM.02.01.01:
"The hospital protects the privacy of health information." *Comprehensive Accreditation Manual for Hospitals (CAMH)*, 2016.

IM.02.01.03:
"The hospital maintains the security and integrity of health information." *Comprehensive Accreditation Manual for Hospitals (CAMH)*, 2016.

RI.01.01.01:
"The hospital respects, protects, and promotes patient rights." *Comprehensive Accreditation Manual for Hospitals (CAMH)*, 2016.

Other Related Accreditation / Regulatory Standards

None.

References

None.

EXHIBIT "B"

THE UNIVERSITY OF TEXAS MD Anderson Cancer Center
Making Cancer History®

MD Anderson Institutional Policy # ADM0389

Disposal of Confidential and/or Sensitive Information Policy

Purpose

The purpose of this policy is to establish the standards for the proper disposal of Confidential and/or Sensitive Information (including, but not limited to, Protected Health Information (PHI)).

Policy Statement

It is the policy of The University of Texas MD Anderson Cancer Center (MD Anderson) to dispose of Confidential and/or Sensitive Information (including PHI) in accordance with applicable legal and regulatory requirements, and through established institutional procedures designed to protect patients, Workforce Members, and the institution.

Scope

Compliance with this policy is the responsibility of all MD Anderson Workforce Members.

Target Audience

The target audience for this policy includes, but is not limited to, all MD Anderson Workforce Members involved in the disposal of Confidential and/or Sensitive Information (including, but not limited to, PHI).

Definitions

Confidential Information: Information of a private nature including, but not limited to:

- Health information records relating to patients, research subjects, and/or employees, including records containing PHI;
- Patient financial records, including but not limited to, account numbers or credit or debit card numbers;
- Personnel and security records, including but not limited to, Social Security numbers, driver's license numbers or other government-issued identification numbers;
- Proprietary information related to research, intellectual property, and scientific discoveries;
- All business and litigation information not deemed a matter of public record; and
- Any other information considered confidential by law.

See also **Data Classification Guidelines and Ratings**.

Protected Health Information (PHI): See **HIPAA Definitions Plan**.

Sensitive Information: Information maintained by the institution that, while not confidential, requires special precautions in order to prevent any disclosure that might harm or embarrass a patient, an employee, or the institution.

Workforce Member: See **HIPAA Definitions Plan**.

Procedure

1.0 Record Retention

1.1 Medical Records:

As appropriate, medical records must be retained in accordance with MD Anderson's **Retention of Official Medical Records Policy (UTMDACC Institutional Policy # ADM0386)**. Questions regarding the retention of Confidential and/or Sensitive Information should be directed to HIM Records Management.

1.2 Other Records:

All other records must be retained in accordance with MD Anderson's **Records Management Policy (UTMDACC Institutional Policy # ADM0107)** and the **Departmental Records Retention Schedules**.

1.3 Retention of outside vendors to perform transportation and/or storage services for records containing PHI must be managed by Supply Chain Management. Any vendor hired to perform transportation and/or storage services for records containing PHI must enter into a Business Associate Agreement with MD Anderson (see MD Anderson's **Business Associate Agreement Policy (UTMDACC Institutional Policy # ADM0342**).

2.0 Disposal

2.1 Paper documents:

A. Documents containing Confidential and/or Sensitive Information (including PHI) that need to be disposed of must be shredded or placed in institutional secured shredding bins. They should not be placed in recycling bins.

B. Only the vendor responsible for transporting and disposing of the contents of the secured shredding bins are allowed to have access to the contents of the secured shredding bins. However, in an emergency situation, a Hospital Administrator may retrieve a document or item from a secured shredding bin. Whether a particular situation constitutes an emergency situation will be determined solely by the Hospital Administrator. Only a Hospital Administrator may access a secured shredding bin for purposes of retrieving a document or item.

C. Questions regarding secured shredding bin placement or maintenance should be directed to Facilities Management, Environmental Health and Safety at 713-563-5000.

2.2 Electronic documents:

A. Confidential and/or Sensitive Information (including PHI) maintained in electronic form must be disposed of in accordance with secure methods of sanitation or destruction approved by the U.S. Department of Health and Human Services (DHHS), Chapter 521 of the Texas Business & Commerce Code, and in accordance with the **Information Resources Security Operations Manual**.

EXHIBIT "B"

B. For assistance in disposing of electronic Confidential and/or Sensitive Information, contact 4-INFO.

2.3 Vendors or contractors hired to transport and/or dispose of records or devices containing Confidential and/or Sensitive Information (including PHI) must execute a Business Associate Agreement and agree to be bound by this policy and all other policies referenced herein.

3.0 Compliance

All Workforce Members not conforming to MD Anderson's **Disposal of Confidential and/or Sensitive Information Policy (UTMDACC Institutional Policy # ADM0389)** are subject to disciplinary action up to and including termination. See **Disciplinary Action Policy (UTMDACC Institutional Policy # ADM0256).**

EXHIBIT "B"

Attachments/Links

Data Classification Guidelines and Ratings.

Departmental Record Retention Schedules.

HIPAA Definitions Plan (Attachment # ATT0699).

Information Resources Security Operations Manual.

Related Policies

Confidentiality Policy (UTMDACC Institutional Policy # ADM0264).

Disciplinary Action Policy (UTMDACC Institutional Policy # ADM0256).

Patient Privacy: Uses and Disclosures of Protected Health Information Policy (UTMDACC Institutional Policy # ADM0401).

Records Management Policy (UTMDACC Institutional Policy # ADM0107).

Retention of Official Medical Records Policy (UTMDACC Institutional Policy # ADM0386).

Business Associate Agreement Policy (UTMDACC Institutional Policy # ADM0342)

Joint Commission Standards / National Patient Safety Goals

“The hospital maintains the security and integrity of health information.” Standard: IM.02.01.03. Comprehensive Accreditation Manual for Hospitals (CAMH), July 2013.

“The hospital protects the privacy of health information.” Standard: IM.02.01.01. Comprehensive Accreditation Manual for Hospitals (CAMH), July 2013.

“The hospital retains its medical records.” Standard: RC.01.05.01. Comprehensive Accreditation Manual for Hospitals (CAMH), July 2013.

Other Related Accreditation / Regulatory Standards

Texas Business & Commerce Code Ch. 521.

U.S. Department of Health & Human Services Guidance for Destruction of PHI, 74 Fed. Reg. 19,006-10 (April 27, 2009).

References

NIST Special Pub. 800-88: Guidelines for Media Sanitization.