

CONFIDENTIAL INFORMATION AND SAFEGUARD INSERT #1 (for use when negotiating agreements that involve the transfer of or access to Customer Information)

[Service Provider] has access to information that pertains to the financial, academic, health, or personal affairs of [MTU], its faculty, staff, students and patients which may be received through any communication or contact (collectively called "Customer Information")¹ in connection with providing services under this Agreement. [Service Provider] will hold the Customer Information in strict confidence and access it only for the explicit business purpose of this Agreement. [Service Provider] will not transfer or disclose the Customer Information to any third party without promptly obtaining the prior written consent of [MTU]'s Office of the General Counsel. In the event of a transfer or disclosure, [Service Provider] will require the recipient of the Customer Information to agree to the same restrictions and conditions that are imposed on the [Service Provider] by this Agreement.

[Service Provider] agrees to comply with all applicable state and federal laws concerning the privacy and confidentiality of the Customer Information. Consequently, [Service Provider] has implemented and will maintain a written comprehensive information security program that includes administrative, technical and physical safeguards for the protection of Customer Information and contains each of the elements set forth in §314.4 of the Gramm Leach Bliley ("GLB") Standards for Safeguarding Customer Information (16 C.F.R. § 314). [Service Provider] further agrees to safeguard all Customer Information in accordance with its information security program and the GLB Standards for Safeguarding Customer Information. [MTU] and any party on behalf of [MTU] may audit [Service Provider's] compliance with the safeguard requirements.

[Service Provider] will report any unauthorized use or disclosure of the Customer Information to [MTU] within one (1) business day after discovering the same. The report will identify (i) the nature of the unauthorized use or disclosure, (ii) the Customer Information used or disclosed, (iii) the person(s) and entities that made the unauthorized use or received the unauthorized disclosure, (iv) actions taken by the [Service Provider] or actions the [Service Provider] will take to mitigate the effect of the unauthorized use or disclosure, and (v) corrective action the [Service Provider] has taken or will take to prevent future similar unauthorized use or disclosure. [Service Provider] will provide such other information, including a written report, as reasonably requested by [MTU].

[Service Provider] will indemnify and hold [MTU] harmless from any and all claims, liabilities, damages, and judgments, including [MTU's] actual costs and actual attorney fees, resulting from the [Service Provider's], its agent's or contractor's failure to comply with the terms of this Agreement.

The confidentiality and information security program requirements provided herein shall survive the termination of this Agreement.

¹Customer Information does not include information which (i) was already in the [Service Provider's] possession prior to disclosure by [MTU] (regardless of whether such disclosure is prior to, on or after the date of this Agreement), (ii) is or becomes generally available to the public other than as a result of a disclosure by the [Service Provider], (iii) becomes available to the [Service Provider] on a non-confidential basis from a source other than [MTU], which source is not prohibited from disclosing the information to the [Service Provider] by a legal, contractual, fiduciary or other obligation to the [Service Provider], (iv) the [Service Provider] can show was independently developed by the [Service Provider] without the use of any Confidential Information of [MTU] or the involvement of any employee of the [Service Provider] who was privy to the Confidential Information of [MTU], or (v) is required by law or regulations to be disclosed.