HIPAA NOTICE OF PRIVACY PRACTICES

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

This HIPAA Notice of Privacy Practices (the "Notice") contains important information regarding your medical information. This Notice is posted on the Insider. You also have the right to receive a paper copy of this Notice and may ask us to give you a copy of this Notice at any time. If you received this Notice electronically, you are entitled to a paper copy of this Notice. If you have any questions about this Notice please refer to the contact information listed in Part 8, below.

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") imposes numerous requirements on employer health plans regarding how certain individually identifiable health information—known as protected health information (or PHI)—may be used and disclosed. This Notice describes how the HIPAA-governed components of the M&T Bank Flexible Benefits Plan (the "Plan"), and any third party that assists in the administration of the Plan, may use and disclose your protected health information for treatment, payment, or health care operations and for other purposes that are permitted or required by law. This Notice also describes your rights to access and control your protected health information. "Protected health information" is information that is maintained or transmitted by the Plan, which may identify you and that relates to your past, present, or future physical or mental health or condition and related health care services.

It is important to note that HIPAA rules apply to the Plan, not M&T as an employer. "We" and "us" as used in this Notice refer to the Plan.

We understand that medical information about you and your health is personal. We are committed to protecting medical information about you and will use it to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request of it. This Notice applies to all of the medical records we maintain. Your personal doctor or health care provider may have different policies or notices regarding their use and disclosure of your medical information.

We are required by law to abide by the terms of this Notice to:

- Make sure that medical information that identifies you is kept private.
- Give you this Notice of our legal duties and privacy practices with respect to medical information about you.
- Follow the terms of the Notice that is currently in effect.

1. HOW WE MAY USE AND DISCLOSE MEDICAL INFORMATION ABOUT YOU.

HIPAA generally permits the use and disclosure of your health information without your permission for purposes of health care treatment, payment activities, and health care operations. These uses and disclosures are more fully described below. Please note that this Notice does not list every use or disclosure; instead it gives examples of the most common uses and disclosures.

- **Treatment:** When and as appropriate, we may use or disclose medical information about you to facilitate medical treatment or services by providers. We may disclose medical information about you to health care providers, including doctors, nurses, technicians, medical students, or other hospital personnel who are involved in taking care of you. For example, we might disclose information about you with physicians who are treating you.

- **Payment:** When and as appropriate, we may use and disclose medical information about you to determine your eligibility for the Plan's benefits, to facilitate payment for the treatment and services you receive from health care providers, to determine benefit responsibility and coverage under the Plan, or to coordinate your coverage. For example, we may disclose information about your medical history to a physician (including your physician) to determine whether a particular treatment is experimental, investigational, or medically necessary, or to decide if the Plan will

cover the treatment. Additionally, we may share medical information with another entity to assist with the adjudication or subrogation of health claims, or with another health plan to coordinate benefit payments.

- **Health Care Operations:** When and as appropriate, we may use and disclose medical information about you for the Plan's operations, as needed. For example, we may use medical information in connection with: conducting quality assessment and administration improvement; underwriting, premium rating, and other activities relating to coverage; conducting or arranging for medical review, legal services, audit services, and fraud and abuse detection programs; business planning and development such as cost management; and business management and general administrative activities of the Plan. For example, we may use your information to review the effectiveness of wellness programs or in negotiating new arrangements with our current or new vendors. We will not use or disclose your genetic information for underwriting purposes.

- **SUD Treatment Information:** If we receive or maintain any information about you from a substance use disorder treatment program that is covered by 42 CFR Part 2 (a "Part 2 Program") through a general consent you provide to the Part 2 Program to use and disclose the Part 2 Program record for purposes of treatment, payment or health care operations, we may use and disclose your Part 2 Program record for treatment, payment and health care operations purposes as described in this Notice. If we receive or maintain your Part 2 Program record through specific consent you provide to us or another third party, we will use and disclose your Part 2 Program record only as expressly permitted by you in your consent as provided to us. In no event will we use or disclose your Part 2 Program record, or testimony that describes the information contained in your Part 2 Program record, in any civil, criminal, administrative, or legislative proceedings by any Federal, State, or local authority, against you, unless authorized by your consent or the order of a court after it provides you notice of the court order.

We will always try to ensure that the medical information used or disclosed is limited to a "Designated Record Set" and to the "Minimum Necessary" standard, including a "limited data set," as defined in HIPAA and ARRA (as defined in Part 3, below) for these purposes. We may also contact you to provide information about treatment options or alternatives or other health-related benefits and services that may be of interest to you.

OTHER PERMITTED USES AND DISCLOSURES

- **Disclosure to Others Involved in Your Care:** We may disclose medical information about you to a relative, a friend, or to any other person you identify, provided the information is directly relevant to that person's involvement with your health care or payment for that care. For example, if a family member or caregiver calls us with prior knowledge of a claim and asks us to help verify the status of a claim, we may agree to help them confirm whether or not the claim has been received and paid.

- **Disclosure to Health Plan Sponsor:** Information may be disclosed to another health plan maintained by M&T Bank for purposes of facilitating claims payments under that plan. In addition, medical information may be disclosed to M&T Bank personnel solely for purposes of administering benefits under the Plan.

- **Workers' Compensation:** We may release medical information about you for workers' compensation or similar programs. These programs provide benefits for work-related injuries or illness.

- **To Comply with Federal and State Requirements:** We will disclose medical information about you when required to do so by federal, state, or local law. For example, we may disclose medical information when required by the U.S. Department of Labor or other government agencies that regulate us; to federal, state, and local law enforcement officials; in response to a judicial order, subpoena, or other lawful process; and to address matters of public interest as required or permitted by law (for example, reporting child abuse and neglect, threats to public health and safety, and for national security reasons). We are

required to disclose medical information about you to the Secretary of the U.S. Department of Health and Human Services if the Secretary is investigating or determining compliance with HIPAA, or to authorized federal officials for intelligence, counterintelligence and other national security activities authorized by law. We may disclose your medical information to a health oversight agency for activities authorized by law (such as audits, investigations, inspections, and licensure).

- To Avert a Serious Threat to Health or Safety: We may use and disclose medical information about you when necessary to prevent a serious threat to your health and safety or the health and safety of the public or another person. Any disclosure, however, would only be to someone who is able to help prevent the threat. For example, we may disclose medical information about you in a proceeding regarding the licensure of a physician.

- Military and Veterans: If you are a member of the armed forces, we may release medical information about you as required by military command authorities. We may also release medical information about foreign military personnel to the appropriate foreign military authority.

- Business Associates: We may disclose your medical information to our business associates. We have contracted with entities (defined as "business associates" under HIPAA) to help us administer your benefits. We will enter into contracts with these entities requiring them to only use and disclose your health information as we are permitted to do so under HIPAA.

- Other Uses: If you are an organ donor, we may release your medical information to organizations that handle organ procurement or organ, eye, or tissue transplantation or to an organ donation bank, as necessary to facilitate organ or tissue donation and transplantation. We may release your medical information to a coroner or medical examiner. If you are an inmate of a correctional institution or under the custody of a law enforcement official, we may release your information to the correctional institution or law enforcement official.

Uses and disclosures other than those described in this Notice will require your written authorization. Your written authorization is required for: most uses and disclosures of psychotherapy notes; uses and disclosures of PHI for marketing purposes; and disclosures that are a sale of PHI. You may revoke your authorization at any time, but you cannot revoke your authorization if the Plan has already acted on it.

The privacy laws of a particular state or other federal laws might impose a more stringent privacy standard. If these more stringent laws apply and are not superseded by federal preemption rules under the Employee Retirement Income Security Act of 1974 (ERISA), the Plan will comply with the more stringent law.

2. YOUR RIGHTS REGARDING MEDICAL INFORMATION ABOUT YOU.

You have the following rights regarding medical information that we maintain about you:

- Right to Inspect and Copy: You have the right to inspect and obtain a copy of your medical information that may be used to make decisions about your benefits under the Plan.

  If you request a copy of the information, we may charge a fee for the costs of copying, mailing, or other supplies associated with your request.

  We may deny your request to inspect and copy in certain very limited circumstances. If you are denied access to medical information, you may request that the denial be reviewed. If the Plan do not maintain the health information, but know where it is maintained, you will be informed of where to direct your request.

- Your Right to Amend: If you feel that medical information we have about you is incorrect or incomplete, you may ask us to amend the information. You have the right to request an amendment for as long as the information is kept by or for the Plan.

  You also must provide a reason that supports your request.

We may deny your request for an amendment if it is not in writing or does not include a reason to support the request. In addition, we may deny your request if you ask us to amend any of the following information:

- Information that is not part of the medical information kept by or for the Plan.
- Information that was not created by us, unless the person or entity that created the information is no longer available to make the amendment.
- Information that is not part of the information which you would be permitted to inspect and copy.
- Information that is accurate and complete.

- **Your Right to an Accounting of Disclosures:** You have the right to request an "accounting of disclosures" (that is, a list of certain disclosures the Plan has made of your health information). Generally, you may receive an accounting of disclosures if the disclosure is required by law, made in connection with public health activities, or in situations similar to those listed above as "Other Permitted Uses and Disclosures". You do not have a right to an accounting of disclosures where such disclosure was made:

- For treatment, payment, or health care operations.
- To you about your own health information.
- Incidental to other permitted disclosures.
- Where authorization was provided.
- To family or friends involved in your care (where disclosure is permitted without authorization).
- For national security or intelligence purposes or to correctional institutions or law enforcement officials in certain circumstances.
- As part of a limited data set where the information disclosed excludes identifying information.

To request this list or accounting of disclosures, you must submit your request, which shall state a time period, which may not be longer than six years and may not include dates before April 14, 2003. Your request should indicate in what form you want the list (for example, paper or electronic). The first list you request within a 12-month period will be free. For additional lists, we may charge you for the costs of providing the list. We will notify you of the cost involved and you may choose to withdraw or modify your request at that time before any costs are incurred.

Notwithstanding the foregoing, you may request an accounting of disclosures of any "electronic health record" (that is, an electronic record of health-related information about you that is created, gathered, managed, and consulted by authorized health care clinicians and staff). To do so, however, you must submit your request and state a time period, which may be no longer than three years prior to the date on which the accounting is requested. In the case of any electronic heath record created on your behalf on or before January 1, 2009, this paragraph shall apply to disclosures made on or after January 1, 2014. In the case of any electronic health record created on your behalf after January 1, 2009, this paragraph shall apply to disclosures made on or after the later of January 1, 2011, or the date we acquired the electronic health record.

- **Your Right to Request Restrictions:** You have the right to request a restriction or limitation on the medical information we use or disclose about you for treatment, payment, or health care operations. You also have the right to request a limit on the medical information we disclose about you to someone who is involved in your care or the payment for your care, like a family member or friend. For example, you could ask that we not use or disclose information about a surgery that you had.

We are not required to agree to your request. If the Plan does agree to a request, a restriction may later be terminated by your written request, by agreement between you and the Plan (including

orally), or unilaterally by the Plan for health information created or received after the Plan has notified you that it has removed the restrictions and for emergency treatment.

To request restrictions, you must make your request in writing and must tell us the following information:

- What information you want to limit.
- Whether you want to limit our use, disclosure, or both.
- To whom you want the limits to apply (for example, disclosures to your spouse).

Effective February 17, 2010 (or such other date specified as the effective date under applicable law), we will comply with any restriction request if: (1) except as otherwise required by law, the disclosure is to the Plan for purposes of carrying out payment or health care operations (and is not for purposes of carrying out treatment); and (2) the protected health information pertains solely to a health care item or service for which the health care provider involved has been paid out-of-pocket in full.

- Right to Request Confidential Communications: You have the right to request that we communicate with you about medical matters in a certain way or at a certain location. For example, you can ask that we only contact you at work or by mail.

  We will not ask you the reason for your request. We will accommodate all reasonable requests. Your request must specify how or where you wish to be contacted.

  You must make any of the requests described above, to the person listed in Part 8, below.

3. BREACH NOTIFICATION.
   Pursuant to changes to HIPAA required by the Health Information Technology for Economic and Clinical Health Act of 2009 and its implementing regulations (collectively, "HITECH Act") under the American Recovery and Reinvestment Act of 2009 ("ARRA"), this Notice also reflects federal breach notification requirements imposed on the Plan in the event that your "unsecured" protected health information (as defined under the HITECH Act) is acquired by an unauthorized party.

   We understand that medical information about you and your health is personal and we are committed to protecting your medical information. Furthermore, we will notify you following the discovery of any "breach" of your unsecured protected health information as defined in the HITECH Act (the "Notice of Breach"). Your Notice of Breach will be in writing and provided via first-class mail, or alternatively, by email if you have previously agreed to receive such notices electronically. If the breach involves:

- 10 or more individuals for whom we have insufficient or out-of-date contact information, then we will provide substitute individual Notice of Breach by either posting the notice on the benefits website on the Insider or by providing the notice in major print or broadcast media where the affected individuals likely reside.
- Less than 10 individuals for whom we have insufficient or out-of-date contact information, then we will provide substitute Notice of Breach by an alternative form.

Your Notice of Breach shall be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and shall include, to the extent possible:

- A description of the breach.
- A description of the types of information that were involved in the breach.
- The steps you should take to protect yourself from potential harm.
- A brief description of what we are doing to investigate the breach, mitigate the harm, and prevent further breaches.
- Our relevant contact information.

Additionally, for any substitute Notice of Breach provided via web posting or major print or broadcast media, the Notice of Breach shall include a toll-free number for you to contact us to determine if your protected health information was involved in the breach.

4. CHANGES TO THIS NOTICE.
   We can change the terms of this Notice at any time. If we do, the new terms and policies will be effective for all of the medical information we already have about you as well as any information we receive in the future. We will send you a copy of the revised notice.

5. COMPLAINTS.
   If you believe your privacy rights have been violated, you may file a complaint with the Plan or with the Secretary of the Department of Health and Human Services. To file a complaint with the Plan, contact the person listed in Part 8, below.

   All complaints must be submitted in writing.

   You will not be penalized for filing a complaint.

6. OTHER USES OF MEDICAL INFORMATION.
   Other uses and disclosures of medical information that are not covered by this Notice or the laws that apply to us will be made only with your written permission. If you grant us permission to use or disclose medical information about you, you may revoke that permission, in writing, at any time. If you revoke your permission, we will no longer use or disclose medical information about you for the reasons covered by your written authorization. You understand that we are unable to take back any disclosures we have already made with your permission, and that we may be required to retain our records related to your benefit determinations and enrollment.

7. EFFECTIVE DATE.
   The effective date of this Notice is January 1, 2027.

8. CONTACT INFORMATION.
   All correspondence relating to the contents of this Notice should be directed to our HR Service Center colleagues at 1-877-473-4732.