



Vendor Privacy & Security Incident Report

Wisconsin Department of Employee Trust Funds
PO Box 7931
Madison WI 53707-7931
1-877-533-5020 (toll free)
Fax 608-267-4549
etf.wi.gov

Use the following form to report any possible or confirmed breaches of protected health information (PHI) or personally identifiable information (PII).

Even if full details are not yet available, the vendor must report any and all known information to ETF within one day of being made aware of a possible breach. Use additional copies of this form to provide additional details as they become known. Reports should be e-mailed to: ETFSMBPrivacyOfficer@etf.wi.gov and ETFSMBInsuranceSubmit@etf.wi.gov.

1. General Information	
1. Your name	
2. Name(s) of person related to reported incident	
3. Incident date	4. Date you first learned of incident
5. Begin date of incident investigation	6. Date of incident report to ETF
7. Current investigation status	
8. Description of documents reviewed in investigation	

2. Incident Information	
1. Was PHI involved? <input type="checkbox"/> Yes <input type="checkbox"/> No, <i>no breach reporting is required under HIPAA.</i> If no, describe the information involved:	
2. Was the PHI involved unsecured? <input type="checkbox"/> Yes <input type="checkbox"/> No, <i>no breach reporting is required under HIPAA.</i> If no, describe the PHI (verbal, paper, electronic, etc.):	
3.1 Was there an acquisition, access, use or disclosure of PHI in a manner not permitted by HIPAA Privacy Rule? <input type="checkbox"/> Yes <input type="checkbox"/> No, <i>no breach reporting is required under HIPAA.</i> <i>Note: A violation of the "minimum necessary" standard is not permitted by the privacy rule. A use or disclosure of PHI that is incident to an otherwise permissible use or disclosure and occurs despite reasonable safeguards and proper minimum necessary procedures is not a violation of the privacy rule.</i>	
3.2 If you answered that an exception applies, skip to section 4.	
Check any/all application boxes below: <input type="checkbox"/> A breach does not include an unintentional acquisition, access or use of PHI by a workforce member, or person acting under the authority of a covered entity or business associate if it was made in good faith <i>and</i> was within the scope of authority <i>and</i> does not result in further use or disclosure in a manner not permitted by the HIPAA Privacy Rule. No breach reporting required under HIPAA. <input type="checkbox"/> A breach does not include an inadvertent disclosure by a person who is authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received is not further used or disclosed in a manner not permitted by the HIPAA privacy rule. No breach reporting required under HIPAA. <input type="checkbox"/> A breach does not include disclosure of PHI where the payer or business associate has a good faith believe that the unauthorized person who received it would not reasonably have been able to retain the information. No breach reporting required under HIPAA. <input type="checkbox"/> No, an exception does not apply; a report to the Office for Civil Rights of the U.S. Department of Health and Human Services is required.	

3. Risk Assessment

1. Describe the number of members impacted and the PHI or PII involved, including the types of identifiers and likelihood of re-identification (if the PHI is de-identified):

2. Describe whether: PHI or PII could be used in a manner adverse to State of Wisconsin members or to further the unauthorized person's interests; and, whether the person or entity that received the PHI or PII has a legal obligation to protect the information.

3. If an electronic breach, describe if the PII or PHI was actually acquired or viewed and attach report from forensic analyst, if available.

4. Describe risk mitigation steps taken:

5. Describe any other relevant factors (write "none" if not applicable):

6. Has your organization determined that there is a low probability that the PHI or PII has been compromised?

Yes, there is a low probability.

No, there is a higher probability that PHI or PII has been compromised, and thus breach reporting is required under HIPAA.

4. Results

1. Summary of findings:

2. Plan of correction:

3. Indicate below any attachments to this notice of, or identify the location of, copies of notices of breach provided to individuals, the media and the Secretary pursuant to your entity's breach notification policy and procedure:

5. Privacy Office Signature

Security officer or privacy official signature

Date

Print name