STATE OF WISCONSIN
Department of Employee Trust Funds
A. John Voelker
SECRETARY

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

Correspondence Memorandum

Date: July 18, 2024

To: Group Insurance Board (Board)

From: Steve Hurley, Director
Office of Policy, Privacy and Compliance

David Maradiaga, Chief Information Security Officer
Bureau of Information Security Management

Renee Walk, Director
Office of Strategic Health Policy

Subject: Vendor Security Framework and Contract Considerations

This memo is for informational purposes only. No Board action is required.

Background

At the May 2024 meeting, the Board voted to temporarily suspend the November 2023 motion to require SOC-2, Type II reports of all vendors contracting with the Board by Dec. 31, 2025. The Board asked that the Department of Employee Trust Funds (ETF) return with alternatives to the SOC-2 in case a vendor was not able to provide a SOC-2 and no adequate vendor alternatives were available.

This memo describes the new process that ETF will implement at the agency level to determine the reporting needed from vendors and how the output from that process will be incorporated into contract negotiations. The memo also discusses how ETF will provide guidance to the Board in instances when a vendor cannot or will not comply with the reporting requirements, as well as when vendors who do report are deemed to be at high risk.

ETF is subject to records confidentiality requirements under state and federal laws that influence contractual arrangements with vendors.

State-Level Privacy Requirements

At the state level there are several privacy laws that apply to ETF's administration of benefits, most notable of which are: Wis. Stat. § 134.98 (Notice of Unauthorized

Pamela L Henning

Reviewed and approved by Pam Henning, Assistant Deputy Secretary
Electronically Signed 07/31/2024

Board	Mtg Date	Item #
GIB	08.14.24	6

Acquisition of Personal Information); 40.07 (Records); and Wis. Admin. Code § ETF 10.70 (Individual Personal Information).

Personally Identifiable Information (i.e., Individual Personal Information) at ETF
Wis. Stat. § 40.07 provides that Individual Personal Information (IPI) is not a public record and may not be disclosed except as provided under the statute. Individual Personal Information covers all information in any individual record of the department but excludes statistical information or other summary information in which individual identification is not possible. See Wis. Admin. Code § ETF 10.70.

Notice of Unauthorized Acquisition of Personal Information (Non-HIPAA Breaches)
Under Wis. Stat. § 134.98, if there is an unauthorized use or disclosure of personal information regarding a non-HIPAA benefit program (such as disability or life insurance), ETF must provide notice to impacted individuals within 45 days of learning of the breach. For a breach involving 1,000 people or more, ETF must, in addition, provide details of the incident to consumer reporting agencies.

Federal-Level Privacy Law (HIPAA)
At the federal level, ETF considers itself to be a Covered Entity under the Health Insurance Portability and Accountability Act's (HIPAA) Privacy Rule regarding the Group Health Insurance Plan, Pharmacy Benefit Plan, and certain other plans administered under Chapter 40, stats. The HIPAA Privacy Rule does not cover all of ETF's business areas. HIPAA is a health insurance law and therefore HIPAA excludes certain types of non-health-insurance activities and plans, such as the retirement plan, deferred compensation, disability/income continuation insurance, life insurance, and accident insurance.

Protected Health Information (PHI) at ETF
HIPAA requires that we safeguard Protected Health Information from unauthorized uses or disclosures. At ETF, PHI means any identifier (e.g., name, address, SSN) linked with health information that is associated with a HIPAA-covered benefit program, such as the State and Local Group Health Insurance Plan, Wellness Program, Pharmacy Benefits, or Dental Insurance (self-insured).

Such information that is not linked to a HIPAA-covered benefit program is not PHI (but could be considered IPI and would still be subject to state laws). These include identifying information associated with the Wisconsin Retirement System, Wisconsin Deferred Compensation Program, Disability/Income Continuation Insurance, Commuter Benefits Program.

HIPAA Business Associates
The HIPAA Privacy Rule requires that any party that performs functions on behalf of, or provides services to, a HIPAA covered entity, that requires the party to receive or access the covered entity's Protected Health Information (PHI), is a Business Associate. If a vendor's services qualify it as a HIPAA Business Associate, it must provide ***written***

satisfactory assurances to the covered entity that the party will appropriately safeguard the PHI that it creates or receives on behalf of the covered entity. Under the Privacy Rule, those ***satisfactory assurances*** are provided to the covered entity via a written contract, known as a Business Associate Agreement (BAA). A BAA specifies each party's responsibilities when it comes to PHI.

For purposes of vendors that meet HIPAA's criteria to be a Business Associate, ETF is compliant with the HIPAA Privacy Rule if the vendor signs a HIPAA-compliant BAA. ETF's Department Terms and Conditions (DTC) contains a HIPAA-compliant BAA. A BAA provides a contractual control and, importantly, ***a HIPAA BAA makes the vendor directly and independently regulated by HIPAA. Review of a vendor's risk analyses and/or monitoring of the vendor is not required under HIPAA.*** However, if ETF becomes aware of a pattern or practice of the Business Associate that is a material breach of the BAA contract, we must take steps to mitigate the situation or terminate the contract, if possible.

Under the changes to the HIPAA Privacy and Security Rules under the federal HITECH Act in 2009, HIPAA Business Associates are subject to enforcement directly under the HIPAA regulation. For example, Business Associates must comply with HIPAA Security Rule requirements to safeguard electronic PHI and conduct regular information risk analyses. See 45 CFR 164.306, 164.308(a)(1)(ii). ("A covered entity or business associate must … conduct an accurate and through assessment of the potential risks and vulnerabilities of the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or the business associate.")

HIPAA-Covered Programs and Areas

GIB Benefit Program/Area	HIPAA-Covered
State/Local Group Health Insurance Plan	Yes
Pharmacy Benefits	Yes
Wellness Program	Yes
Dental Insurance (Self-Insured)	Yes
Health Savings Accounts	Yes
Health Reimbursement Accounts/FSA	Yes
DAISI Data Warehouse	Yes
Long Term Care Insurance (Employee Pay-All)	Yes*

GIB Benefit Program/Area	HIPAA-Covered
Vision Insurance (Employee Pay-All)	Yes*
Dental (Employee Pay-All)	Yes*
Board Actuaries	Yes
Accident Insurance (Employee Pay-All)	No
Long Term Disability Insurance	No
Income Continuation Insurance	No
Group Life Insurance	No

*ETF provides no PHI to these programs. However, the administrators of these benefits are already regulated by HIPAA as to information of members who choose to enroll.

Vendor Risk Management Framework
ETF has developed a third-party cybersecurity risk management framework built upon the National Institute of Standards and Technology (NIST) standards to assess the risk exposure incurred as a part of conducting contracted services. The framework will initially assess the inherent vendor risk profile to determine the grouping of cybersecurity controls to be measured. The cybersecurity controls being assessed correlate to a variety of regulatory requirements and security standards, such as HIPAA and other data privacy standards, and in many cases exceed the requirements of law. The framework will be used across all vendors who use or have access to private member data.

ETF will require the vendors to provide a report to demonstrate the effectiveness of the controls initially identified. The framework does not prescribe the type of report but is focused on the output of the controls necessary for ETF security staff to measure the effectiveness of the vendors cybersecurity defenses that safeguard member information. The SOC-2 is an example of a report that would (in most cases) meet the highest level of control reporting needs. ETF is open to other reports so long as the information provided is sufficient and addresses the appropriate controls based on the type of data the vendor has about ETF members.

Post-Framework Risk Scoring
After ETF determines the level of reporting needed, the vendor will provide the report demonstrating the effectiveness of their controls, ETF information security staff will review the report, request additional information as needed, and provide a risk-based score dependent on the findings after the report is reviewed. ETF staff will classify the

risk identified in vendors cyber security practices according to three risk level assignments—low, medium, or high.

ETF will report the initial findings of all risk management reports in November of each year and will report on vendors that are being considered as part of procurement as final vendor decisions are made.

Vendors Unable to Report
In some cases, a vendor may not be able to provide the level of reporting that the assessment framework indicates should be provided. In these cases, ETF will attempt to negotiate alternate means of access to the necessary information to assure controls are in place. If negotiations are unsuccessful, ETF will bring this information to the Board, along with other considerations, such as:

- How crucial is this specific vendor to providing the service in question? Are similar services available from other vendors?
- What are the financial risks to the program if the Board contracts with this vendor? If they don't?
- Are there reputational risks to the Board and/or ETF in contracting with this vendor, given the potential security gaps that may be present?
- Are there options to mitigate potential risks (e.g., contracting considerations, cyber insurance, etc.)?

Vendors with Medium or High-Risk Scores
If a vendor who is currently under contract and providing adequate reporting receives a medium- or high-risk score due to the findings in the report, ETF will work with the vendor to establish a plan for correcting findings, with regular communications from the vendor on progress. ETF will report on the vendor's corrective action plan when initial findings are reported in November and will provide periodic updates to the Board as appropriate, either to notify them of progress or of a lack of progress that indicates greater corrective action may need to be taken.

Application of Framework
ETF will use the framework to evaluate reporting needs for all vendors, with a goal of evaluating all vendor contracts by December 2025. For vendors with in-force contracts that will extend past December 2025, ETF will compare the evaluated need versus reporting already being provided and determine whether changes to reporting should be negotiated as a part of the next contract renewal.

In the case of procurements (i.e., requests for proposals, invitations to bid) already released by the Board, ETF will use the framework to guide what level of reporting will be requested as part of negotiations. As mentioned earlier in this memo, vendors who provide a SOC-2, Type II report will typically meet the required level of reporting. ETF issued an addendum to the most recent Request for Proposals to clarify that proposers

who do not currently have a SOC-2 report could submit “other alternative independent service auditor report(s), including attestation that clearly articulates and demonstrates the overall design and operating effectiveness of the Proposer’s internal controls, coverage period testing, subservice organizations, and the specific systems and services to be used in the delivery of services to the Department for consideration.” ETF will use the framework internally to help evaluate such submissions.

Staff will be at the Board meeting to answer any questions.