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: October 20, 2023

To: Group Insurance Board

From: David Maradiaga, Chief Information Security Officer
Ruth Ballard, Security Analyst
Bureau of Information Security Management

Subject: Minimum Baseline Information Technology Security Standards

The Department of Employee Trust Funds (ETF) staff request the Group Insurance Board (Board) approval to add requirements to vendor contracts that clarify that alternatives to System and Organization Controls (SOC) 2 submissions must provide to ETF detailed visibility into the health plans security controls — scope, description, evaluation criteria, and results.

Background

As an ongoing operational effort, ETF collected the annual independent service auditor's report within the SOC 2, Type 2 audit or a Health Information Trust Alliance (HITRUST) certificate from all Health and Benefit plans to provide the Board with the results of our analysis.

ETF requested information system security audits for calendar year 2022 from the one Medicare Advantage provider and ten fully insured health plan providers contracted with the Board to offer State of Wisconsin Group Health Insurance Program (GHIP) coverage to employees and retirees of state agencies, University of Wisconsin System, University of Wisconsin Hospitals & Clinics Authority, and participating local government employees.

ETF staff from the Bureau of Information Security Management (BISM) and the Office of Strategic Health Policy (OSHP) coordinated with health plans on the submission of their annual System and Organization Controls (previously referred to as Service Organization Controls) audit report, corresponding Bridge Letter, where applicable, and/or equivalent documentation.

ETF's security assessors rely on the independent auditors report in the SOC 2 to provide detailed visibility into the health plans IT security controls — scope, description, evaluation criteria, and results. The report is designed to help the external recipient of the report assess the risks arising from interactions with the vendor's system,

Pamela L Henning

Reviewed and approved by Pam Henning, Assistant Deputy Secretary
Electronically Signed 11/10/2023

Board	Mtg Date	Item #
GIB	11.15.23	21

particularly the risks to the security, availability, processing integrity, confidentiality, and privacy of their information.

In contrast, the HITRUST certificate is external, but the HITRUST Full Report is internal and not intended for external recipients. It is specific to HIPAA and HIPAA-related activities. It does not enable ETF to assess Third Party IT Security overall, which includes all other related activities, such as how the systems and applications where member data resides are protected or how data that may (or may not) be classified as HIPAA is accessed, maintained, processed, stored, or transmitted. The HITRUST certificate does not tell us which trust service principles are in scope or the level of testing performed (e.g., criteria of population, sample sizes, exceptions, management responses, or plan of actions to address those gaps). The HITRUST certification does not tell us which (if any) subservice organizations are in use or the vendor's management oversight performed.

With a SOC 2 Report, auditors are required to follow-up on any exceptions from prior years. This does not occur with the HITRUST Certificate. The SOC 2 covers a consecutive 6–12-month period, while the HITRUST is just a certificate of achievement reassessed once every two years for a point in time. Furthermore, a HITRUST certification does not communicate end-user controls, so ETF program managers know what ETF must do to ensure we have the applicable controls in place. It is simply a certificate. A detailed report is provided to the customer organization requesting the HITRUST assessment. However, it is limited to HIPAA related functions and does not necessarily target systems and delivery of services to ETF.

Summary of Health Plan Submissions

Overall, all but one health plan provided a SOC 2, Type 2 report providing the needed visibility for them to demonstrate compliance with the audit provision, as outlined in the Department Terms and Conditions. One provided a Health Information Trust Alliance HITRUST certificate, which provided very limited visibility and could not demonstrate compliance with needed audit provisions and, as such, was deemed to be an elevated risk.

ETF staff from BISM and OSHP were able to coordinate a meeting with the health plan, which submitted the HITRUST certificate. Our ETF security assessors were able to glean some of the necessary detail to provide limited assurances of their security controls and the maturity of their information risk management practices.

Recommendation to Improve Ongoing Submissions

It is ETF's recommendation that the Board include a contract provision which requires health plans to maintain or pursue SOC 2, Type 2 reports. A deadline for compliance should be included in the contract. If a health plan fails to submit a SOC 2 Type 2 report (submission of a HITRUST certificate) as they pursue compliance, ETF will require the health plan to allow further examination of their security practices. For example, ETF could require nonconforming health plans to accommodate (within 30 days notification) a minimum, four-hour, live screen showing of their full HITRUST Report for examination by relevant ETF staff (e.g., BISM program manager). This examination would allow ETF to assess the independent auditor's detailed testing approach; the testing results; and follow-up on their policies, standards, and procedures, including full disclosure and oversight of their subservice organizations.

This approach will allow ETF more visibility into the scope, description, evaluation and results in the design, suitability, and operational effectiveness of internal controls. This will lead to a better assessment on how well to health plans protect the systems and applications used to access, maintain, process, store, and transmit member data.

ETF will continue to work with all contracted health plans to improve overall audit submission compliance and improve visibility into information security risk in future plan years.

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