



Department of Employee Relations
City of Milwaukee

**BREACH OF INFORMATION
FREQUENTLY ASKED QUESTIONS**

November 20, 2013, Revised 11/25/13

Revised 12/6/13

1. When was the City of Milwaukee notified of the incident involving the theft of City of Milwaukee employee information from a Dynacare employee? Why were employees not notified immediately?

The Department of Employee Relations was notified the afternoon of Friday November 15, 2013. Given the seriousness and implications of the information received, the Department of Employee Relations immediately notified the City Attorney's Office and the Mayor's Office as well as the President of the Common Council, the Chair of the Finance and Personnel Committee, and the Police and Fire Departments. A communication to employees was drafted and sent at the end of the business day on Friday November 15th, the same day the City learned of the breach.

2. What exact information has been compromised?

According to the information we have received from Dynacare Laboratories, the flash drive stolen contained a database with patient demographic information, which included patient names, Social Security numbers, addresses, dates of birth, and gender of City employees. Since the City is not aware of exactly which employees were included in the database used by the Dynacare worker, we have to assume that the information of all benefit eligible employees, spouses and domestic partners may have been compromised. This includes information from employees who don't participate in the Wellness Program AND employees who waive the City's health insurance.

The City therefore recommends that all benefit eligible employees, spouses, and domestic partners take steps to protect their identity and monitor their accounts.

NOTE: Employees can verify if their protected information was included in the breach by calling Dynacare at 1-877-237-4971, Monday – Friday, 9:00 am to 5:00pm.

- Although there have been some reports that social security numbers for spouses and domestic partners were not part of the breach, it appears that some social security numbers for those individuals were included in the original file given to Froedtert Workforce Health in a secure, password protected manner. Spouses and domestic partners who receive the letter from Dynacare should assume that their information was compromised. (Updated 11/25/13)*
- The City never provided any information to Dynacare directly. The City provided employee, spouse, and domestic partner information to Froedtert Workforce Health in a secured, password protected format. The information included social security numbers for the purpose of matching the release of test results to the appropriate employees. The City expected Froedtert Workforce Health and its subcontractors to comply with the privacy and security rules under HIPAA and with the terms of the contract with the City in protecting the security of that information. (Updated 11/25/13)*
- Employees who were benefit eligible as of May of 2013 and who subsequently separated (retired, resigned, or were discharged) may have received a letter from Dynacare informing them that their information has been compromised. The City recommends that those former employees take advantage of the offer as long as they received a letter because the City is not 100% sure of whose information has been compromised given Dynacare's access to Froedtert's information. The City will also be notifying those separated employees of the situation as they have not received any communication from the City and may not be aware that the Dynacare letter had important information for them. (Added 12/06/13)*

3. Was the information of employees of the Housing Authority (HACM) and Milwaukee Economic Development Corporation (MEDC) included in the breach? (Added 12/06/13)

The City is in the process of determining if information on HACM and MEDC employees was compromised. HACM and MEDC employees who have not received a letter from Dynacare should contact 1-877-237-4971 to determine, according to Dynacare records, if their information has been compromised.

4. Why was the employee's Social Security number used by the City when the employee information was provided to Froedtert Workforce Health? (Added 11/25/13)(Revised 12/06/13)

The Social Security number was provided to Froedtert Workforce Health to ensure that the test results were appropriately matched and distributed to the right individuals participating in the Program. All employee information was provided to Froedtert Workforce Health in a secure and password protected manner. The City is looking at alternative options to accomplish this objective in the future. It is important to note that the City used employee social security numbers for a lawful purpose: the administration of employee benefits. This lawful use did not require prior notification to the employees.

5. Does the Department of Employee Relations use an employee's social security number for other benefits administration purposes? (Added 12/06/13)

Yes, DER uses employee social security numbers for other benefit administration purposes as required by law for health insurance administration purposes, worker's compensation reporting to the state, and identity and employment eligibility purposes at time of hire. DER is completing an audit of other uses of social security numbers for other benefit applications and will eliminate other uses of this information that are not required by law effective as soon as administratively feasible.

6. Why was the information of employees who waive the City's health insurance or don't participate in the Wellness Program included in the information provided to Froedtert Workforce Health? (Added 11/25/13)

The information provided to Froedtert Workforce Health included information on benefit eligible employees who may sign up for health insurance and/or participate in the Wellness Program. At the time the information is provided to Froedtert Workforce Health, the City does not know who will enroll and who will participate in the Program for the next year/cycle.

7. Was the information of children who are dependents compromised? (Added 11/25/13)

No, dependent information was not provided to Froedtert Workforce Health so there is no potential for their information to be compromised.

8. Was any medical or financial information compromised?

No, according to Dynacare Laboratories no other information was included in the database.

9. Given the breach of this confidential information, aren't all employees, spouses, and domestic partners victims of identity theft?

No. The breach by itself does not constitute identity theft. If someone has attempted to use or used your personal identifying information, other than just your name, to obtain money, goods, services or credit, without your consent, you may be the victim of identity theft. Employees who are victims of identity theft should follow the procedures identified in the FAQ Identity Theft – What to do if you are the Victim of Identity Theft available from the DER website.

10. What are the definitions of a “breach” and “unsecured protected health information” under HIPAA? (Added 11/25/13)

A breach means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under the law which compromises the security or privacy of the protected health information. Unsecured Protected Health Information means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology.

11. How is a Dynacare health care worker allowed to have access to this type of private employee information?

The City does not know the details of how or why the employee was in possession of this information.

Dynacare has stated to the media that the employee was in possession of a flash drive with employee information because the City required their employees to perform work in conjunction with the Wellness Program in remote locations and that they did not have adequate connectivity to permit remote access. The City was not aware of any connectivity issues communicated by Dynacare. Furthermore that reason does not justify Dynacare’s decision to allow the personal information of 6,000 employees and 3,000 spouses to be stored in an unsecured format. (Updated 11/25/13)

12. What is Dynacare doing as a result of this incident?

According to a statement released by Dynacare, they are conducting a comprehensive internal review of their policies and procedures and re-enforcing education to their employees on the importance of safeguarding patient information.

*A dedicated line has been established by Dynacare for City employees who have questions about the incident. The number is 1-877-237-4971, Monday - Friday, 9:00 am to 5:00pm. All City employees whose information was compromised will be receiving a letter from Dynacare Laboratories later this week with information about a one-year free membership in “ProtectMyID Alert” an identity theft notification program. The letter will contain instructions on how to activate your membership. Your spouse or domestic partner will need to call separately. **If you have not received the letter, you can call the number above and identify yourself as a City of Milwaukee employee. Ask the representative to verify if your information was compromised. You will be given instructions on how to proceed if your information was compromised.***

13. What is included with the membership in ProtectMyID Alert?

We have been provided with information that indicates that as a result of the membership, eligible employees will be provided with a free copy of their Experian credit report, daily monitoring of suspicious activity on their Experian, Equifax, and TransUnion credit reports, access to a dedicated Identity Theft Resolution Agent (if employees are in fact the victims of identity theft), and access to an insurance policy that can help cover certain costs incurred as a result of the identity theft. Please refer to Dynacare letter for specifics.

14. Do employees who activate their free membership per Dynacare’s offer also have to place Fraud Alerts with the credit reporting agencies? (Added 12/06/13)

Initial Fraud Alerts stay in your file for at least 90 days. This Initial Security Alert alerts credit grantors to verify your identity in case someone is using your information without your consent. The same services are available through ProtectMyID for one year.

15. Is the City accepting Dynacare’s offer for one year of free membership in ProtectMyID Alert as a settlement of the breach of protected information?

No, Dynacare has offered the membership in conjunction with their original response to the incident and the breach. However, the City is committed to identifying and pursuing all options that are in the interest of the employees and that provide appropriate protection and response given the seriousness of this action and the potential for identity theft.

16. Does an individual who signs up for ProtectMyID waive any future rights to take action against anyone? *No.*

17. Many employees feel that one year of protection offered by Dynacare is not enough, what is the City doing about this? (Added 11/25/13)

The City is looking at all viable options, legal and other to protect employees from identity theft given the breach.

18. If someone uses my credit card, is it considered identity theft? (Added 11/25/13)

No. If your card provider refunds your account, you are not the victim of identity theft, but you should file a police report for lost/stolen credit card with the MPD by calling 933-4444. However, if a known person has stolen your card you need to file a police report in person at a district station.

19. Is there an incident report number that employees can use if they want to place a freeze of their credit or to file an extended alert with one of the three consumer reporting agencies in addition to signing up for ProtectMyID Alert? (Added 11/25/13) (Revised 12/06/13)

No, the Milwaukee Police Department has not issued an incident report for the breach of personal information. A determination will be made as to when to issue such report when there is evidence of actual fraudulent activity that can be tied to the breach of information. If and when an incident report number is available, employees will be notified immediately. (Revised 12/06/13)

20. Why shouldn't the City terminate the contract with Dynacare? (Added 11/25/13)

The City does not have a contract with Dynacare. The City's contract is with Froedtert Workforce Health. The City is investigating all viable options given the breach.

21. What actions is the City pursuing as a result of this action?

The City is currently:

- *identifying and implementing all options available to educate employees of steps they can take to prevent identity theft and providing information about the actions needed if and when someone becomes the victim of identity theft;*
- *conducting an investigation of the circumstances of the incident and the delay in the notification process;*
- *requesting a full description of measures in place at Froedtert Health Workforce Health and required of their subcontractors for protecting the integrity, confidentiality, and availability of protected client information created, received, held or transmitted.*
- *reviewing the terms and conditions of the existing contract with Froedtert Health Workforce Health and exploring all options; and,*
- *reviewing all internal procedures associated with the use, storage, and or transmission of private employee information.*

After consultation with members of the Common Council and the Mayor, the Office of the City Attorney has decided to file a formal complaint with the federal Office of Civil Rights against Dynacare Laboratories for its admitted breach of HIPAA security requirements regarding the private information of more than 9,000 City of Milwaukee employees, their spouses and their domestic partners. This action follows Dynacare's recent filing of a notice of breach of unsecured protected health information, its apparent unwillingness to communicate or cooperate with city representatives or to release details of its investigation, its failure to provide information to the city in order to protect our employees and the misleading comments Dynacare provided to the media.(Updated 11/25/13)

22. What does the filing of the complaint by the City with the Office of Civil Rights mean? (Added 11/25/13)

It means that the City on behalf of its employees is asking the Office of Civil Rights Compliance to investigate a violation of HIPAA's privacy rule given Dynacare's filing of a notice of breach of unsecured protected health information with the Wisconsin's Office of Privacy Protection.

23. Where can employees find Dynacare's notice of breach? (Added 11/25/13)

http://datcp.wi.gov/Consumer/Office_of_Privacy_Protection/Data_Breaches/index.aspx

24. What is the future of the City's Wellness Program? (Added 11/25/13)(Revised 12/06/13)

At this time, policy makers and Elected Officials are assessing the future of the Program. Given that there is a pending investigation, it is premature to try to answer that question with any level of certainty. The members of the City's Labor Management Committee have expressed a strong desire to recognize the value of a Wellness Program. They are committed to identifying and implementing the necessary changes to ensure an effective and secure program in the future given this breach. This includes considering a different vendor, if necessary. (Revised 12/06/13)

25. What is the status of the Outcomes-based component recently approved by the Common Council given this incident? (Added 12/06/13)

On 12/04/13 the Finance and Personnel Committee adopted a resolution directing the Department of Employee Relations to take the appropriate steps necessary to suspend the outcomes-based component of the City's Wellness Program in light of the breach of information associated with Dynacare Labs and Workforce Health. This component related to an employee's eligibility to receive a \$150 contribution to a Health Reimbursement Account based on achieving optimal lab values, improvement in certain lab values from the previous year, and activities related to improved lab values.

26. Should employees who have not completed Step 3 of the Wellness Program go through with their scheduled appointments and coaching sessions? (Added 11/25/13)(Revised 12/06/13)

Yes, employees who intended to complete all phases of the Wellness Program should in fact continue with their plans. Information regarding the future of the Program for 2014 and beyond will be distributed when available.

Employees who fail to complete the meeting with the health coach will be treated as non participants and will be assessed the 2014 non-participant fee accordingly. (Revised 12/06/13)

27. Where should employees send questions and concerns regarding the incident?

City employees, spouses and domestic partners with questions and concerns should send an email to the Department of Employee Relations at mmonte@milwaukee.gov or mbrady@milwaukee.gov. DER will use your questions and concerns to update this document and follow up as necessary. Employees who are victims of identity theft should follow the procedures identified in the FAQ Identity Theft – What to do if you are the Victim of Identity Theft available from the DER website.

28. Where can employees get the most current information regarding the incident and other relevant information?

The Department of Employee Relations is committed to maintaining employees informed with the most up to date information that is available to the extent allowable given the pending investigation and potential legal ramifications. This information will be posted on the DER website as it becomes available.