OAKLAWN HOSPITAL

Email Compromise
Frequently Asked Questions

---

1. What happened?

Oaklawn Hospital recently learned that, as a result of a phishing email, an unauthorized party obtained access to a limited number of employee email accounts between April 14, 2020 and April 15, 2020. Oaklawn Hospital immediately contained the impacted accounts and commenced a prompt and thorough investigation. As part of its investigation, Oaklawn Hospital worked very closely with external cybersecurity professionals. After an extensive forensic investigation and comprehensive manual document review, we discovered on July 28, 2020 that one or more of the accessed email accounts contained some of your protected health information.

Oaklawn Hospital has no evidence that any of your information has been misused. Nevertheless, out of an abundance of caution, Oaklawn Hospital wants to make you aware of the incident and offer our assistance.

2. How did this happen?

As a result of a phishing email, an unauthorized party obtained access to a limited number of employee email accounts.

3. What information was specifically impacted?

It is important to note that we have no evidence that information related to this incident has been misused. The information involved includes patient names, dates of birth, various medical and health insurance information, and, in a very limited number of cases, Social Security numbers, financial account information, driver's license numbers, and online login information. The letter you received explains the information impacted for you. This incident does not affect all patients of Oaklawn Hospital.

4. What are you doing for me?

Oaklawn Hospital is taking several steps in this matter. The company is notifying all appropriate authorities and communicating by letter with potentially affected patients. We are advising patients to monitor statements from healthcare providers and insurance companies to ensure that all the services listed on their statements were, in fact, performed on their behalf and notify the appropriate authority if they see anything suspicious. We have created a dedicated, toll-free response line to answer questions about this incident. Finally, Oaklawn Hospital is offering complimentary credit monitoring to those limited individuals whose Social Security number was included in the impacted accounts.

5. Who is behind this attack?

Our investigation is still ongoing.

6. How did you discover this?

Oaklawn Hospital identified suspicious e-mails in a limited number of employee email accounts. We engaged outside cybersecurity experts to work with our internal team. Together, they determined Oaklawn Hospital was the victim of a phishing attack.

7. How could you let this happen?

Oaklawn Hospital takes its responsibility to protect the information it maintains seriously. Unfortunately, no one is immune from phishing attacks. While there were already security measures in place to protect individuals' information, Oaklawn Hospital took prompt action to remedy the situation. We regret any inconvenience or concern this may cause you. Oaklawn Hospital has no evidence that any specific personal information was in fact misused.

8. Who is Oaklawn Hospital?

Oaklawn Hospital and Medical Group is an independently owned, not-for-profit hospital and general medical service provider located in Marshall, Michigan. It serves the medical needs of the residents of Calhoun County and greater south-central Michigan.

9. Why does Oaklawn Hospital have my information?

In connection with medical services you received at Oaklawn Hospital, you provided certain personal and protected health information to Oaklawn Hospital.

10. If this occurred in April, why am I only hearing about it now?

Our team has worked diligently since this incident was discovered. This investigation included a comprehensive forensic investigation and labor-intensive manual review of records. We are confident we moved as quickly as possible in this matter.

11. It appears as if this information was stolen from an email. Was this information encrypted? If not, why?

Our investigation is ongoing. Despite there being known access to the impacted email accounts, we have no evidence that the threat actor viewed or accessed any of your information in those accounts.

12. How do I know if I was impacted? If I do not receive a letter, does that mean I am not involved in this incident/notification?

Letters were mailed on September 25, 2020. If you do not receive a letter in the next few weeks, you may not be a part of this notification. If you did not receive a notice letter and you think you may be impacted, please provide your full name, and I will confirm whether your information may have been compromised as a result of this incident.

13. What information of mine specifically was impacted? How can you be sure?

The letter you received describes the information of yours that was impacted. The information involved includes patient names, dates of birth, various medical and health insurance information, and, in a very limited number of cases, Social Security numbers, financial account information, driver's license numbers, and online login information. This incident does not affect all patients of Oaklawn Hospital and not all of these elements were included for each notified individual. We have no evidence that information related to this incident has been misused.

14. Was my protected health information included?

The protected health information impacted by this incident was patient names, dates of birth, various medical and health insurance information, and, in a very limited number of cases, Social Security numbers, financial account information, driver's license numbers, and online login information.

15. Was my Social Security number included?

This information was involved only if indicated in your notice letter.

16. Was my Driver's License number included?

This information was involved only if indicated in your notice letter.

17. Was my state identification number included?

This information was involved only if indicated in your notice letter.

18. Was my credit/debit account information included?

This information was involved only if indicated in your notice letter.

19. Was my bank account information involved?

This information was involved only if indicated in your notice letter.

20. Was my protected health information included?

Your letter states specifically what information of yours may have been included in this incident.

21. Did anyone gain access to my patient portal information or actual medical record/electronic health record (EHR)?

No. The unauthorized individual only gained access to the limited employee email accounts.

22. How many individuals were potentially impacted? Is anyone impacted in [specific state or country]?

The total number of individuals whose information may have been accessed as a result

of this incident is approximately 26,861. This number represents only a portion of all patients for whom Oaklawn Hospital provides service.

23. I see reports online that 26,861 individuals are potentially impacted. How did you arrive at this number?

The total number of individuals whose information may have been accessed as a result of this incident is 26,861. This number represents only a portion of all patients for whom Oaklawn Hospital provides service.

24. Why was my personal information in an employee's email account?

In the healthcare industry it is sometimes necessary for employees to have patient information in their email inboxes to resolve customer service inquiries, or for billing purposes. Oaklawn Hospital ensures that employees who have access to patient information fully understand and comply with HIPAA privacy laws. Oaklawn Hospital has no evidence that any of the information has been acquired or used by any unauthorized individual, but out of an abundance of caution, we are notifying impacted individuals so they can take steps to protect themselves.

25. What is a phishing campaign?

A phishing campaign is an email scam designed to obtain personal information from individuals by disguising the identity of the email sender as a trustworthy organization or reputable person.

26. What has the unauthorized person done with my information?

To date, Oaklawn Hospital has no evidence that any of the information has been misused. Nevertheless, out of an abundance of caution, Oaklawn Hospital wants to make you aware of the incident, provide you with guidance on what you can do to protect yourself, and to let you know that Oaklawn Hospital continues to take significant measures to protect your information.

27. As a result of this incident, will I become a victim of identity theft?

To date, Oaklawn Hospital has no evidence that any of the information has been misused. Out of an abundance of caution, Oaklawn Hospital wants to make you aware of the incident, provide you with guidance on what you can do to protect yourself, let you know that it continues to take significant measures to protect your information, and finally, offer you protection at no cost to you. For the vast majority of patients being notified, the information affected was very limited and is unlikely to lead to identity theft.

28. Should I close my credit or debit account?

If your notice letter indicates that your credit or debit account may have been impacted, Oaklawn Hospital recommends that you contact your financial institution to inquire about steps you can take to protect your account, including whether your account should be cancelled or whether you should obtain a new card. Regardless of whether your credit or debit account information was impacted, Oaklawn Hospital recommends you remain

vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

29. What can I do to protect myself?

Oaklawn Hospital suggests you consider taking the following steps:

- Enroll in the credit monitoring services offered at no cost to you, if eligible.
- You should always remain vigilant in reviewing your financial and credit/debit card account statements for fraudulent or irregular activity on a regular basis.
- You may consider placing a fraud alert and/or security freeze on your credit file.
- You may order a free credit report.
- Follow the steps provided in your notice letter to safeguard yourself against medical identity theft.

30. Why did I not receive a notice about this incident?

Oaklawn Hospital provided notice via U.S. Mail to all those potentially impacted. If you did not receive a notice letter and you think you may be impacted, please provide your full name and name and phone number, we will do our best to confirm whether your information may have been compromised as a result of this incident. If it is determined that your information may have been compromised, someone call you back to discuss.

31. Is Oaklawn Hospital providing credit monitoring services?

Yes, Oaklawn Hospital is offering credit monitoring through Experian® for individuals whose Social Security numbers were included in the impacted accounts.

32. How do I enroll in Experian IdentityWorks Credit 3B?

If your Social Security number was impacted, Oaklawn Hospital is providing you with a complimentary one-year membership in Experian IdentityWorks Credit 3B at no cost to you. The service is provided by Experian, one of the three major nationwide credit reporting companies. You can enroll at https://www.experianidworks.com/credit or by calling 877.288.8057. You will use the 9-character Activation Code included with your notification letter. Further instructions for enrolling are included with your notification letter. The deadline to enroll is December 21, 2020. A credit card is not required to enroll.

33. What happens after I enroll in Experian IdentityWorks Credit 3B?

As soon as you enroll in Experian's® IdentityWorks Credit 3B, Experian will begin to monitor your Experian, Equifax, and TransUnion credit reports, and will automatically alert you of key changes to your credit report. You also will have access to your Credit Report. The service includes up to $1 Million in identity theft insurance. (Certain policy limitations and exclusions may apply.) After the expiration of the one-year free subscription, you will have an option to renew Experian's® credit monitoring product at your own cost if you choose to do so.

Once your enrollment in IdentityWorks Credit 3B is complete, you should carefully review your credit report for inaccurate or suspicious items. If you have any questions about IdentityWorks Credit 3B, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877.288.8057.

34. What is included in Experian IdentityWorks Credit 3B?

- Experian credit report at signup: See what information is associated with your credit file. Daily credit reports are available for online members only.
- Credit Monitoring: Actively monitors Experian file for indicators of fraud.
- Experian IdentityWorks ExtendCARETM: You receive the same high level of Identity Restoration support even after your Experian IdentityWorks membership has expired at no additional cost to you.
- $1 Million Identity Theft Insurance: Provides coverage for certain costs and unauthorized electronic fund transfers.

35. Why did I receive two years of credit monitoring? (alternatively, Why did I only receive one year of credit monitoring?)

For individuals whose Social Security number was included, Oaklawn Hospital has provided the length of credit monitoring that is required by applicable law and by best practices.

36. Can Oaklawn Hospital just register me in the credit monitoring product?

Unfortunately, Oaklawn Hospital cannot register for you. You must enroll yourself online (or over the phone) using the Activation Code in your notice letter if you received one. If you need assistance, I can put you in touch with someone who can help guide you through the process.

37. How long do I have to enroll in the credit monitoring product?

You can sign up for this service anytime between now and December 21, 2020 using the Enrollment Code listed in your notification letter.

38. Why am I being asked for my Social Security Number to enroll in these services?

You do need to provide some personal information to allow for the monitoring of your credit. Experian will use this information to provide you with the identity theft protection and credit monitoring services being offered.

39. Why is Oaklawn Hospital <u>NOT</u> offering me credit monitoring?

Oaklawn Hospital is offering credit monitoring to those individuals whose Social Security number was in the accessed accounts. If the letter you received does not specifically mention Social Security number, then the information belonging to you that was impacted by this incident is not of a type that typically results in identity theft.

40. What is a fraud alert?

A fraud alert tells creditors to contact you personally before they open any new accounts.

41. How do I place a fraud alert on my account?

In order to place a fraud alert, you will need to call any one of the three major credit bureaus (as soon as one credit bureau confirms your fraud alert, they will notify the others to place fraud alerts). Alternatively, you may file the Fraud Alert online. Here is a link to the Experian fraud alert home page: https://www.experian.com/fraud/center.html

Equifax	**Experian**	**TransUnion**
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
www.equifax.com	www.experian.com	www.transunion.com
1-800-525-6285	1-888-397-3742	1-800-680-7289

42. How long does a fraud alert last?

An initial fraud alert lasts one year and there is no cost to you; you may then renew the fraud alert for an additional 90 days.

43. Will a fraud alert stop me from using my credit cards?

No. A fraud alert will not stop you from using your credit cards or other accounts.

44. Can I still apply for a credit card after I place a fraud alert on my credit report?

Yes, but the verification process may be more cumbersome. Potential creditors will receive a message alerting them to the possibility of fraud and that creditors should re-verify the identity of a person applying for credit.

45. How do I place a Security Freeze on my credit files and how much does it cost?

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file, at no cost to you. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by sending a request in writing, by mail, to all three nationwide credit reporting companies. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion Security Freeze**
PO Box 105788	PO Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
https://www.freeze.equifax.com	http://experian.com/freeze	www.transunion.com/securityfreeze
1-800-685-1111	1-888-397-3742	1-800-680-7289

In order to place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a

unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name, or to commit fraud or other crimes against you, you may file a police report in the City in which you currently reside.

[NOTE – PLEASE VERIFY THAT THE CALLER IS ELIGIBLE FOR CREDIT MONITORING BEFORE READING THE NEXT PARAGRAPH.]

If you do place a security freeze *prior* to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring. After you sign up for the credit monitoring service, you may refreeze your credit file.

46. What should I do if I find suspicious activity on my credit reports or have reason to believe my information is being misused?

Promptly call your local law enforcement agency and file a police report. Get a copy of the police report, as many creditors will want the information it contains to absolve you of fraudulent debts. You may also file a complaint with the FTC at www.ftc.gov/idtheft or reach the FTC at 1-877-IDTHEFT (1-877-438-4338) or 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcers for their investigations.

47. When I called to place a fraud alert, they asked for my Social Security number. Is this ok?

Yes. The credit bureaus will indeed ask for your Social Security number and other personal information to verify your identity and avoid sending any credit report or correspondence to the wrong individual. However, Oaklawn Hospital cautions against providing any information to any entity or person *contacting you directly* asking for your personal information.

48. How do I obtain a free credit report?

Under federal law, you are entitled to one free credit report every 12 months from each of the three major nationwide credit reporting companies. Call 1-877-322-8228 or request your free credit reports online at www.annualcreditreport.com. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

49. I lost my notification. Can you provide a new one to me?

Yes. Please confirm your name and address and Oaklawn Hospital will ensure that you receive another notification if you are confirmed to be potentially impacted.

50. I have experienced fraud on my payment card. What do I do?

If you see a fraudulent charge on your payment card, you should immediately contact the bank, credit union or other financial institution that issued your card. The phone number to call can be found on the back of the card. If reported promptly, major credit card companies typically guarantee cardholders will not be responsible for fraudulent charges.

51. Is this letter legitimate? Is it a scam?

I can assure you the letter is legitimate. Safeguarding information is a top priority for Oaklawn Hospital. Oaklawn Hospital wants to make you aware of the situation so you can take steps to protect yourselves, and to provide you with guidance on how you can protect yourself.

52. Do I have any legal recourse?

Unfortunately, Oaklawn Hospital is not in a position to provide any legal advice related to the incident.

53. Has the unauthorized individual been identified or caught?

Oaklawn Hospital is not aware that the unauthorized individual has been identified or caught. Oaklawn Hospital's primary focus remains on supporting those individuals who were impacted by this incident.

54. Will we receive any additional information or update?

If a further update is warranted, Oaklawn Hospital will provide one accordingly.

55. The individual this letter is addressed to is deceased. What should I do?

The letter includes recommended actions you can take to protect the deceased's identity..

56. I have additional questions that cannot be answered. What should I do?

Please provide me with your full name and contact information and we will have a representative contact you within forty-eight (48) hours during business hours. If you are calling on behalf of someone else, please provide the name of the person that the letter was addressed to.

57. Who are you (Call Center)?

We are a vendor of Oaklawn Hospital and we are managing this incident response line for them.