Notice of Data Privacy Incident

1. **What happened?**
   We became aware of a security incident on November 11, 2025. The investigation determined that an unauthorized actor gained access to certain files within our systems from November 9 -11, 2025. Importantly, we continued caring for patients throughout our response to the incident, and have resumed normal operations.

   Upon learning of the situation, Issaqueena Dentistry immediately took steps to contain and remediate the incident, activated incident response protocols, and launched an internal investigation. We also reported the incident to law enforcement. The ongoing investigation recently determined that the unauthorized third party acquired and/or accessed certain files on the organization's network.

2. **When did this happen?**
   An unauthorized actor gained access to certain parts of our systems from November 9-11, 2025.

3. **What information about me may have been involved?**
   We are currently in the process of conducting a detailed review of these files to determine whether personal information or protected health information was present within the affected files and to whom the information relates. This process is time-intensive, but ultimately necessary to properly identify potentially affected individuals.

4. **Was this a ransomware attack?**
   Yes.

5. **Did you pay a ransom?**
   Due to the confidential nature of the investigation into this event, we are not able to provide additional details.

6. **Are your systems secure?**
   Issaqueena Dentistry has taken several steps to secure their systems and currently has no evidence to suggest any ongoing threat to their network.

7. **Who was the threat actor? / Who carried out this attack on Issaqueena Dentistry?**
   Due to the confidential nature of the investigation into this event, we are not able to provide additional details.

8. **How many patients were affected?**
   The data review is ongoing, and I do not have that information at this time.

9. **Have the police been/local authorities been notified? If so, with which police department and what is the case number?**
   The event was reported to law enforcement. We continue to work with law enforcement on their ongoing investigation.

10. **How can I have my information removed from the server/directory?**
    We are not able to remove this information. We must maintain certain patient and employment data as part of our data retention policies and as required by law.

11. **Why didn't you tell affected individuals about the loss of the data sooner?**
    Investigations like this take time to complete, and we are committed to a thorough review alongside our third-party experts. We are taking this incredibly seriously and depending on our findings from the

data review, we may follow this notice by sending letters to affected individuals at the mailing address we have on file in accordance with applicable laws.

12. **What is Issaqueena Dentistry doing to prevent this kind of loss from happening again?** We value the trust our patients, employees and colleagues place in us to protect the privacy and security of their information, and we sincerely regret any inconvenience or concern this incident has caused. For our part, we are continuing to work with third-party experts to enhance our technical security measures.

13. **What is the deadline for registering for the pre-paid package of identity protection services?** The call center can be reached at 844-525-5119, Monday through Friday, between 9 am and 5 pm Eastern Time, except holidays. The enrollment deadline is currently set for May 2, 2026.

14. **I heard about the incident in the media, but I did not receive a letter. Was my information compromised? When will I receive a letter?**
Our investigation is ongoing, and we are continuing to review the data involved in this incident. At this point, we have not been able to determine whose personal information or protected health information has been affected.

    As an added precaution, Issaqueena Dentistry is offering complimentary access to identity monitoring, fraud consultation, and identity theft restoration services to help mitigate any potential for harm at no cost. We encourage individuals to contact IDX with any questions and to enroll in free identity protection services by calling 844-525-5119. IDX representatives are available Monday through Friday from 9:00 am to 5:00 pm Eastern Time. Please note the deadline to enroll is May 2, 2026. Individuals can also visit Issaqueena Dentistry's website for more information at www.issaqueenadental.com

    Depending on our findings from the data review, in addition to the website notice, we may send written notice to impacted individuals directly in accordance with applicable laws.

What You Can Do To Protect Your Minor's Personal Information

Avoiding Medical ID Theft. The following practices can provide additional safeguards to protect against medical identity theft.

- Regularly check the accounts you use regularly to pay for health-related expenses, including bank accounts, health savings accounts, credit card accounts.
- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.
- Review your "explanation of benefits statement" which you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize.

Review Personal Account Statements and Credit Reports. We recommend that you remain vigilant by reviewing personal account statements and monitoring your/ your minor's credit reports to detect any errors or unauthorized activity. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To

obtain a free annual credit report, go to www.annualcreditreport.com or call (877) 322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months. If you discover any suspicious items, you should report any incorrect information on your report to the credit reporting agency. The names and contact information for the credit reporting agencies are:

Report Suspected Fraud. You have the right to file a police report if your minor experience's identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You should report suspected incidents of identity theft to local law enforcement, your state's Attorney General, and/or the Federal Trade Commission.

Place Fraud Alerts. Add a fraud alert statement to your minor's credit file (if one exists) at all three national credit-reporting agencies: Equifax, Experian, and TransUnion. This statement alerts creditors of possible fraudulent activity within your report as well as requests that they contact you prior to establishing any accounts in your minor's name. Once the fraud alert is added to your minor's credit report, all creditors should contact you prior to establishing any account in your minor's name. You only need to contact one of the three agencies listed below; your request will be shared with the other two agencies. To place a fraud alert, contact the nationwide credit reporting agencies by phone or online. For more information, visit https://www.consumer.ftc.gov/articles/0275-place-fraud-alert.

Place a Security Freeze. . Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator or have a valid power of attorney, you can get a free freeze for that person, too. To place a security freeze, contact the nationwide credit reporting agencies by phone or online. If you request a freeze online or by phone, the agency must place the freeze within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets your request. You also can lift the freeze temporarily without a fee. Also, do not confuse freezes with locks. They work in a similar way, but locks may have monthly fees. If you want a free freeze guaranteed by federal law, then opt for a freeze, not a lock. For more information, visit https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs.

Obtain additional information about the steps you can take to avoid identity theft from the following entities:

- **All U.S. Residents:** The Identity Theft Clearinghouse, Federal Trade Commission may be contacted at 600 Pennsylvania Avenue, NW Washington, DC 20580; 1-877-IDTHEFT (438-4338); and www.consumer.ftc.gov. This notification was not delayed by law enforcement.