

[Cross Timbers Letterhead]

[First Name] [Last Name]

[Address 1]

[Address 2]

[City] [State] [Zip Code]

[Date]

**Re: Notice of Security Incident**

Dear [Name]:

Cross Timbers Health Clinics, Inc. d/b/a AccelHealth (“Accel”) is writing to inform you of an event that may impact the privacy of some of your personal information. While we are unaware of any attempted or actual misuse of your information, we are providing you with information about the event, our response, and steps you may take to protect against any misuse of your information, should you feel it necessary to do so.

**What Happened?** On or about December 15, 2021, Accel discovered it could not access certain files on its servers. Upon discovery of the event, Accel immediately launched an investigation with the assistance of third-party computer forensics specialists. The investigation determined that certain systems had been infected by malware which prevented access to some files on the network. The investigation also determined that certain files within Accel’s network could have been subject to unauthorized access between December 9, 2021 and December 15, 2021. Accel then took steps to conduct a review of the files to ensure we identified all individuals with information potentially at risk, as well as to identify contact information for those individuals. That process was completed on January 14, 2022. Although Accel is unaware of any actual or attempted misuse of individuals’ information, Accel is providing notice of this incident to those individuals whose information was potentially impacted.

**What Information Was Involved?** The impacted information related to you which may be impacted includes your name, address, date of birth, Social Security number, driver’s license number, financial account information, health insurance information, medical record number, and treatment/diagnosis information. We have no evidence your information was subject to actual or attempted misuse.

**What We Are Doing.** We take this incident and the security of personal information in our care very seriously. As part of our ongoing commitment to the privacy of information in our care, we are implementing additional technical security measures designed to mitigate recurrence of this type of incident. We are also reviewing and enhancing existing data privacy policies and procedures.

As an added precaution we are offering you access to twelve months of credit monitoring and identity theft protection services through IDX at no cost to you. If you wish to activate these services, you may follow the instructions included in the attached *Steps You Can Take to Help Protect Your Personal Information*. We encourage you to enroll in these services as we are unable to act on your behalf to do so.

**What You Can Do.** We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and explanation of benefits forms and monitoring your free credit reports for suspicious activity and to detect errors. We also encourage you to review the *Steps You Can Take to Help Protect Your Personal Information* section of this letter.

**For More Information.** If you have questions about this incident that are not addressed in this letter, please contact us at [number] from [times].

Sincerely,

AccelHealth

## STEPS YOU CAN TAKE TO PROTECT YOUR PERSONAL INFORMATION

### Enroll in Identity Monitoring Services

[Credit/Identity Monitoring Instructions]

### Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

<b>Equifax</b>	<b>Experian</b>	<b>TransUnion</b>
<a href="https://www.equifax.com/personal/credit-report-services/">https://www.equifax.com/personal/credit-report-services/</a>	<a href="https://www.experian.com/help/">https://www.experian.com/help/</a>	<a href="https://www.transunion.com/credit-help">https://www.transunion.com/credit-help</a>
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

### Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; [www.identitytheft.gov](http://www.identitytheft.gov); 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You

have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

*For District of Columbia residents*, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and [oag@dc.gov](mailto:oag@dc.gov).

*For Maryland residents*, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and [www.oag.state.md.us](http://www.oag.state.md.us). Accel is located at 1100 W. Reynosa Ave, De Leon, TX 76444.

*For New Mexico residents*, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting [www.consumerfinance.gov/f/201504\\_cfpb\\_summary\\_your-rights-under-fcra.pdf](http://www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf), or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

*For New York residents*, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov/>.

*For North Carolina residents*, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and [www.ncdoj.gov](http://www.ncdoj.gov).

*For Rhode Island residents*, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; [www.riag.ri.gov](http://www.riag.ri.gov); and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are [#] Rhode Island residents impacted by this incident.

# **EXHIBIT B**

## ***NOTICE OF DATA PRIVACY INCIDENT***

Cross Timbers Health Clinics, Inc. d/b/a AccelHealth (“Accel”) is providing notice of a recent incident that may affect the security of information pertaining to individuals, including certain current and former patients and employees. The confidentiality, privacy, and security of information in Accel’s care is one of its highest priorities and Accel takes this incident very seriously. Although Accel has not received any reports of actual or attempted misuse of the impacted personal information, Accel is providing this notice in an abundance of caution.

***What Happened?*** On or about December 15, 2021, Accel discovered it could not access certain files on its servers. Upon discovery of the event, Accel immediately launched an investigation with the assistance of third-party computer forensics specialists. The investigation determined that certain systems had been infected by malware which prevented access to some files on the network. The investigation also determined that certain files within Accel’s network could have been subject to unauthorized access between December 9, 2021, and December 15, 2021. Accel then took steps to conduct a review of the files to ensure we identified all individuals with information potentially at risk, as well as to identify contact information for those individuals. That process was completed on January 14, 2022. Although Accel is unaware of any actual or attempted misuse of individuals’ information, Accel is providing notice of this incident to those individuals whose information was potentially impacted.

***What Information Was Involved?*** The impacted information which may have been impacted varied by individual but included name, address, date of birth, Social Security number, driver’s license number, financial account information, health insurance information, medical record number, and treatment/diagnosis information. We have no evidence your information was subject to actual or attempted misuse.

***What We Are Doing.*** Accel takes this incident and the security of personal information in our care very seriously. As part of our ongoing commitment to the privacy of information in our care, we are implementing additional technical security measures designed to mitigate recurrence of this type of incident. We are also reviewing and enhancing existing data privacy policies and procedures. As an added precaution, Accel is offering credit monitoring for individuals whose information was impacted.

***For More Information.*** We understand some people may have additional questions concerning this incident. Individuals can direct questions to 1-833-783-1447, Monday through Friday from 8 am to 8 pm Central Time.

***What You Can Do.*** Accel encourages you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and explanation of benefit forms, and monitoring your free credit reports for suspicious activity and to detect errors. Accel apologizes for any inconvenience this may cause and remains committed to the privacy and security of all information it maintains.

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which

is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

<b>Equifax</b>	<b>Experian</b>	<b>TransUnion</b>
<a href="https://www.equifax.com/personal/credit-report-services/">https://www.equifax.com/personal/credit-report-services/</a>	<a href="https://www.experian.com/help/">https://www.experian.com/help/</a>	<a href="https://www.transunion.com/credit-help">https://www.transunion.com/credit-help</a>
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; [www.identitytheft.gov](http://www.identitytheft.gov); 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

# **EXHIBIT C**

**CROSS TIMBERS HEALTH CLINICS PROVIDES NOTICE  
OF DATA PRIVACY INCIDENT**

**DeLeon, TX – February 7, 2022** – Cross Timbers Health Clinics d/b/a AccelHealth (“Accel”) today is providing information about a recent event that may impact the privacy of some personal data related to current and former patients and employees. The confidentiality, privacy, and security of information in Accel’s care is one of its highest priorities and Accel takes this incident very seriously. Although Accel has not received any reports of actual or attempted misuse of the impacted personal information, Accel is providing this notice in an abundance of caution.

***What Happened?*** On or about December 15, 2021, Accel discovered it could not access certain files on its servers. Upon discovery of the event, Accel immediately launched an investigation with the assistance of third-party computer forensics specialists. The investigation determined that certain systems had been infected by malware which prevented access to some files on the network. The investigation also determined that certain files within Accel’s network could have been subject to unauthorized access between December 9, 2021, and December 15, 2021. Accel then took steps to conduct a review of the files to ensure Accel identified all individuals with information potentially at risk, as well as to identify contact information for those individuals. That process was completed on January 14, 2022. Although Accel is unaware of any actual or attempted misuse of individuals’ information, Accel is providing notice of this incident to those individuals whose information was potentially impacted.

***What Information Was Involved?*** The impacted information which may have been impacted varied by individual but included name, address, date of birth, Social Security number, driver’s license number, financial account information, health insurance information, medical record number, and treatment/diagnosis information. We have no evidence any information was subject to actual or attempted misuse.

***What We Are Doing.*** Accel takes this incident and the security of personal information in our care very seriously. As part of Accel’s ongoing commitment to the privacy of information in its care, Accel is implementing additional technical security measures designed to mitigate recurrence of this type of incident. Accel is also reviewing and enhancing existing data privacy policies and procedures. As an added precaution, Accel is offering credit monitoring for individuals whose information was impacted.

***For More Information.*** We understand some people may have additional questions concerning this incident. Individuals can direct questions to 1-833-783-1447, Monday through Friday from 8 am to 8 pm Central Time.

***What You Can Do.*** Accel encourages you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and explanation of benefits forms, and monitoring your free credit reports for suspicious activity and to detect errors. Accel apologizes for any inconvenience this may cause and remains committed to the privacy and security of all information it maintains.

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before

extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

<b>Equifax</b>	<b>Experian</b>	<b>TransUnion</b>
<a href="https://www.equifax.com/personal/credit-report-services/">https://www.equifax.com/personal/credit-report-services/</a>	<a href="https://www.experian.com/help/">https://www.experian.com/help/</a>	<a href="https://www.transunion.com/credit-help">https://www.transunion.com/credit-help</a>
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; [www.identitytheft.gov](http://www.identitytheft.gov); 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.