



February [XX], 2018

[Name]  
[Address 1]  
[Address 2]  
[City, State Zip]

## **NOTICE OF DATA BREACH**

Dear [Name]:

FastHealth was or is a contracted vendor of [entity]. We provide healthcare clients with operational and website services. We are committed to protecting the security and confidentiality of personal information. Regrettably, we are writing to notify you of a security incident that may have involved some of your information that you submitted through an online form at the hospital's website. This notice explains the incident, measures we have taken and some additional steps that you can take in response.

### **What Happened?**

On November 2, 2017, FastHealth received a report from law enforcement indicating that an unauthorized third party may have accessed or acquired certain information from FastHealth databases. We immediately began an investigation and hired a leading computer security firm to assist with the investigation. The investigation determined that, in mid-August 2017, an unauthorized third party was able to access FastHealth's web server and may have been able to acquire information from certain databases.

### **What Information Was Involved?**

We undertook a comprehensive review of the information in the databases involved, which analysis was completed on January 26, 2018, and determined that the information includes your name<<data elements>>.

### **What You Can Do.**

To date, we have no indication that any of your personal information has been misused in any way. As a precaution, **we have secured the services of Kroll to provide identity monitoring at no cost to you for one year.** Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit <<IDMonitoringURL>> to activate and take advantage of your identity monitoring services.  
*You have until <<Date>> to activate your identity monitoring services.*  
Membership Number: <<Member ID>>

To receive credit services by mail instead of online, please call 1-???-???-???. Additional information describing your services as well as more information on ways to protect yourself are included.

### **What We Are Doing.**

To help prevent this type of incident from occurring again, we are implementing a new encryption solution for sensitive personal information that we store and maintain, and we are strengthening our data protection and security protocols.

### **For More Information.**

If you have any questions, please call [call center number] from [hours of operation].

We sincerely apologize for any inconvenience or concern this incident may cause you.

Sincerely,

A handwritten signature in blue ink, appearing to read "Kevin A. Foote". The signature is fluid and cursive, with the first name "Kevin" and last name "Foote" clearly legible.

Kevin A. Foote  
Founder & CEO



You have been provided the opportunity to access the following services<sup>1</sup> from Kroll:

### **Single Bureau Credit Monitoring**

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

### **Fraud Consultation**

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

### **Identity Theft Restoration**

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you.

## **MORE INFORMATION ON WAYS TO PROTECT YOURSELF**

Even if you choose not to take advantage of the complimentary credit monitoring, we remind you to remain vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

*Experian*, PO Box 2002, Allen, TX 75013, [www.experian.com](http://www.experian.com), 1-888-397-3742  
*TransUnion*, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://www.transunion.com), 1-800-916-8800  
*Equifax*, PO Box 740241, Atlanta, GA 30374, [www.equifax.com](http://www.equifax.com), 1-800-685-1111

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

*Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue, NW Washington, DC 20580, 1-877-IDTHEFT (438-4338), [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)

If your health insurance information is involved in this incident, we recommend that you review the explanation of benefits that you receive from your health insurer. If you see services that you did not receive, please contact your insurer immediately.

---

<sup>1</sup> Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

February [XX], 2018

[Name]

[Address 1]

[Address 2]

[City, State Zip]

## **NOTICE OF DATA BREACH**

Dear [Name]:

FastHealth was or is a contracted vendor of [entity]. We provide healthcare clients with operational and website services. We are committed to protecting the security and confidentiality of personal information. Regrettably, we are writing to notify you of a security incident that may have involved some of your information that you submitted through an online form at the hospital's website. This notice explains the incident, measures we have taken and some additional steps that you can take in response.

### **What Happened?**

On November 2, 2017, FastHealth received a report from law enforcement indicating that an unauthorized third party may have accessed or acquired certain information from FastHealth databases. We immediately began an investigation and hired a leading computer security firm to assist with the investigation. The investigation determined that, in mid-August 2017, an unauthorized third party was able to access FastHealth's web server and may have been able to acquire information from certain databases.

### **What Information Was Involved?**

We undertook a comprehensive review of the information in the databases involved, which analysis was completed on January 26, 2018, and determined that the information includes your name<<data elements>>.

### **What You Can Do.**

To date, we have no indication that any of your personal information has been misused in any way. We encourage that you remain vigilant to the possibility of fraud and identity theft by reviewing your financial statements for any unauthorized activity. You should immediately report any unauthorized charges to your financial institution because the major credit card companies have rules that restrict them from requiring you to pay for fraudulent charges that are timely reported. The phone number to call is usually on the back of your payment card. You should also review the additional information on the following page on ways to protect yourself.

### **What We Are Doing.**

To help prevent this type of incident from occurring again, we are implementing a new encryption solution for sensitive personal information that we store and maintain, and we are strengthening our data protection and security protocols.

### **For More Information.**

If you have any questions, please call [call center number] from [hours of operation].

We sincerely apologize for any inconvenience or concern this incident may cause you.

Sincerely,



Kevin A. Foote  
Founder & CEO

## **MORE INFORMATION ON WAYS TO PROTECT YOURSELF**

We remind you to remain vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

*Experian*, PO Box 2002, Allen, TX 75013, [www.experian.com](http://www.experian.com), 1-888-397-3742  
*TransUnion*, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://www.transunion.com), 1-800-916-8800  
*Equifax*, PO Box 740241, Atlanta, GA 30374, [www.equifax.com](http://www.equifax.com), 1-800-685-1111

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

*Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue, NW Washington, DC 20580, 1-877-IDTHEFT (438-4338), [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)



February [XX], 2018

Parent or Guardian of [Name]  
[Address 1]  
[Address 2]  
[City, State Zip]

## **NOTICE OF DATA BREACH**

Dear Parent or Guardian of [Name]:

FastHealth was or is a contracted vendor of [entity]. We provide healthcare clients with operational and website services. We are committed to protecting the security and confidentiality of personal information. Regrettably, we are writing to notify you of a security incident that may have involved some of your child's information that you submitted through an online form at the hospital's website. This notice explains the incident, measures we have taken and some additional steps that you can take in response.

### **What Happened?**

On November 2, 2017, FastHealth received a report from law enforcement indicating that an unauthorized third party may have accessed or acquired certain information from FastHealth databases. We immediately began an investigation and hired a leading computer security firm to assist with the investigation. The investigation determined that, in mid-August 2017, an unauthorized third party was able to access FastHealth's web server and may have been able to acquire information from certain databases.

### **What Information Was Involved?**

We undertook a comprehensive review of the information in the databases involved, which analysis was completed on January 26, 2018, and determined that the information includes your child's name<<data elements>>.

### **What You Can Do.**

To date, we have no indication that any of your child's personal information has been misused in any way. To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide Fraud Consultation and Identity Theft Restoration at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data.

Your **child's** Membership Number is: <<**Member ID**>>

Additional information describing your **child's** services is included with this letter.

If you have questions, please call **1-???-???-????**, Monday through Friday from **8:00 a.m. to 5:00 p.m. Central Time**. Please have your child's membership number ready.

Protecting your **child's** information is important to us. We trust that the services we are offering to you demonstrate our continued commitment to your security and satisfaction.

### **What We Are Doing.**

To help prevent this type of incident from occurring again, we are implementing a new encryption solution for sensitive personal information that we store and maintain, and we are strengthening our data protection and security protocols.

### **For More Information.**

If you have any questions, please call [call center number] from [hours of operation].

We sincerely apologize for any inconvenience or concern this incident may cause you.

Sincerely,

A handwritten signature in blue ink, appearing to read "Kevin A. Foote". The signature is fluid and cursive, with the first name "Kevin" and last name "Foote" clearly legible.

Kevin A. Foote  
Founder & CEO



You have been provided the opportunity to access the following services from Kroll:

### **Fraud Consultation**

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your child's identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

### **Identity Theft Restoration**

If your child becomes a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you.

### **MORE INFORMATION ON WAYS TO PROTECT YOURSELF**

Even if you choose not to take advantage of the complimentary services, we remind you to remain vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

*Experian*, PO Box 2002, Allen, TX 75013, [www.experian.com](http://www.experian.com), 1-888-397-3742

*TransUnion*, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://www.transunion.com), 1-800-916-8800

*Equifax*, PO Box 740241, Atlanta, GA 30374, [www.equifax.com](http://www.equifax.com), 1-800-685-1111

If you believe you or your child are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

*Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue, NW Washington, DC 20580, 1-877-IDTHEFT (438-4338), [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)