14875

Health
Recovery Services
Where Change & Recovery Begin

<<Date>> (Format: Month Day, Year)

<<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

Dear <<FirstName>> <<LastName>>,

We write to inform you of a recent event that could potentially affect the security of some of your personal and health information. While we are unaware of any actual or attempted misuse of such information, Health Recovery Services, Inc. ("HRS") takes this incident very seriously. Out of an abundance of caution, we are providing you with information and access to resources so that you can better protect your information, should you feel it is appropriate to do so.

**What Happened?** On February 5, 2019, we discovered that our computer network had been accessed by an unauthorized IP address. We immediately launched an investigation into the nature and scope of this access and disconnected our network and information systems. We also moved to rebuild our entire network to ensure it was secure and free of any security threat. On March 15, 2019, our third-party forensic expert determined that the unauthorized access to our network occurred from November 14, 2018 until its discovery on February 5, 2019. While the forensic expert has indicated to us that they do not believe that any of HRS' patient information was ever in fact accessed, they were unable to definitively rule out that possibility.

**What Information Was Involved?** While our investigation is ongoing, we have no evidence that the unknown third party accessed or acquired protected health information stored on the HRS server. Nevertheless, we confirmed this server stored files and a software application which may have contained your name, address, phone number, and date of birth. If you were a patient of HRS after 2014, the information stored in the files and software application also included your medical information, health insurance information, diagnosis, and treatment information. Out an abundance of caution, we are providing notice of this incident to you given we cannot rule out unauthorized access to this information occurred.

**What We Are Doing.** HRS is committed to protecting the confidentiality and security of all the information in our possession. We have security measures, policies, and procedures in place to help protect your data and we continue to review these measures as part of our ongoing commitment to the security of the information in our care. In addition to launching the ongoing investigation and restoring the integrity of our entire network, we are reviewing our policies and procedures and enhancing the security of our information systems to help prevent an incident like this from occurring in the future.

**What Can You Do?** 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.

Please review the enclosed "Steps You Can Take to Protect Against Identity Theft and Fraud." This section provides additional information about how to protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file. This section also includes a description of the services HRS is offering and how to enroll. We encourage you to enroll in these services, as we are not able to act on your behalf to activate your identity monitoring services.

**For More Information.** We understand you may have questions relating to this event and this letter. We established a dedicated assistance line staffed with individuals familiar with this incident and how to better protect against the possibility of identity theft and fraud. You can direct all questions and concerns to this line by calling 1-833-231-3360, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time. Please have your membership number ready.

We apologize for any inconvenience this incident may cause you and remain committed to the privacy and security of our client information.

Sincerely,

Regina Smith, MBA
Chief Financial Officer
Health Recovery Services, Inc.

## Steps You Can Take to Protect Against Identity Theft and Fraud

To help relieve concerns and restore confidence following this incident, 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 **my.idmonitoringservice.com** to activate and take advantage of your identity monitoring services.

*You have until **July 4, 2019** to activate your identity monitoring services.*

Membership Number: <<Member ID>>

To receive credit services by mail instead of online, please call 1-833-231-3360. Additional information describing your services is included with this letter.

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security 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 security 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 security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

**Experian**
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

**TransUnion**
P.O. Box 2000
Chester, PA 19016
1-888-909-8872
www.transunion.com/credit-freeze

**Equifax**
P.O. Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
www.equifax.com/personal/credit-report-services

In order to request a security freeze, you may need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior 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, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your 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 agencies listed below:

**Experian**
P.O. Box 2002
Allen, TX 75013
1-888-397-3742
www.experian.com/fraud/center.html

**TransUnion**
P.O. Box 200
Chester, PA 19016
1-800-680-7289
www.transunion.com/fraud-victim-resource/place-fraud-alert

**Equifax**
P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008
www.equifax.com/personal/credit-report-services

You can review helpful sites to learn more about consumer protection related to information compromise, i.e. AHIMA's *Medical Identity Theft Response Checklist for Consumers*, which can be found at http://bit.ly/2pHDcqV.

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

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); 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.

Do not provide any personal information to anyone requesting information from you by telephone or e-mail. Be wary of scams that may appear to offer protection but are really trying to get personal information from you. If you have any suspicions about the authenticity of an e-mail or text, do not click the links in it. Please call HRS directly if you are unsure.

**For Maryland residents**, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us.

Kroll | A Division of DUFF&PHELPS

## TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services[1] 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. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

[1] 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.

# EXHIBIT C

14875

Health
Recovery Services
Where Change & Recovery Begin

## NOTICE OF DATA INCIDENT

**April 5, 2019**

Health Recovery Services, Inc. ("HRS") is posting this statement on our website as a precautionary measure and as part of our commitment to patient privacy. HRS takes our patients' privacy seriously, and it is important to us that you are made fully aware of a recent incident which potentially involves personal information of HRS' current and past patients.

***What Happened?*** On February 5, 2019, we discovered that our computer network had been accessed by an unauthorized IP address. We immediately launched an investigation into the nature and scope of this access and disconnected our network and information systems. We also moved to rebuild our entire network to ensure it was secure and free of any security threat. On March 15, 2019, our third-party forensic expert determined that the unauthorized access to our network occurred from November 14, 2018 until its discovery on February 5, 2019. While the forensic expert has indicated to us that they do not believe that any of HRS' patient information was ever in fact accessed, they were unable to definitively rule out that possibility.

***What Information Was Involved?*** While our investigation is ongoing, we have no evidence that the unknown third party accessed or acquired protected health information stored on the HRS server. Nevertheless, we confirmed this server stored files and a software application which may have contained demographic information such as name, address, phone number, and date of birth. If you were a patient of HRS after 2014, the information stored in the files and software application may also have included medical information, health insurance information, diagnosis, and treatment information. For certain patients, these files may also have contained Social Security numbers. Out an abundance of caution, we are providing notice of this incident to any individual that may be affected by the data event given we cannot rule out unauthorized access to this information occurred.

***What Health Recovery Services Is Doing.*** HRS is committed to protecting the confidentiality and security of all the information in our possession. HRS has security measures, policies, and procedures in place to protect its data and continues to review these measures as part of its ongoing commitment to the security of the information held in its care. In addition to launching the ongoing investigation and restoring the integrity of its entire network, HRS is reviewing its policies and procedures and enhancing the security of its information systems to mitigate the risk an incident like this will occur in the future.

***What You Can Do.*** We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus.

To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security 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 security 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 security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

| Experian | TransUnion | Equifax |
|---|---|---|
| PO Box 9554 | P.O. Box 2000 | PO Box 105788 |
| Allen, TX 75013 | Chester, PA 19016 | Atlanta, GA 30348-5788 |
| 1-888-397-3742 | 1-888-909-8872 | 1-800-685-1111 |
| www.experian.com/freeze/center.html | www.transunion.com/credit-freeze | www.equifax.com/personal/credit-report-services |

In order to request a security freeze, you may need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior 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, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your 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 agencies listed below:

| Experian | TransUnion | Equifax |
|---|---|---|
| P.O. Box 2002 | P.O. Box 2000 | P.O. Box 105069 |
| Allen, TX 75013 | Chester, PA 19016 | Atlanta, GA 30348 |
| 1-888-397-3742 | 1-800-680-7289 | 1-888-766-0008 |
| www.experian.com/fraud/center.html | www.transunion.com/fraud-victim-resource/place-fraud-alert | www.equifax.com/personal/credit-report-services |

You can review helpful sites to learn more about consumer protection related to information compromise, i.e. AHIMA's *Medical Identity Theft Response Checklist for Consumers*, which can be found at http://bit.ly/2pHDcqV.

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

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); 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.

We are keenly aware of how important our patients' personal information is to them, and we apologize for any inconvenience. We are committed to providing quality care, including protecting our patients' personal information. We have been working with our forensic expert and our IT team to review and analyze the security of our computer systems, and we have updated certain technical, administrative and physical safeguards to ensure the security and confidentiality of your data in the future.

If you have any questions, please call our toll-free dedicated assistance line staffed with individuals familiar with this incident and how to better protect against the possibility of identity theft and fraud has been established by HRS. You can direct all questions and concerns to this line by calling 1-833-231-3360, between 8:00 a.m. and 5:30 p.m. Central Time, Monday through Friday.