

**LEWIS
BRISBOIS
BISGAARD
& SMITH LLP**
ATTORNEYS AT LAW

1055 Westlakes Drive, Suite 300
Berwyn, Pennsylvania 19312
Telephone: 215.977.4100
Fax: 215.977.4101
www.lewisbrisbois.com

LAURA A. RIEBEN
DIRECT DIAL: 215.977.4066
LAURA.RIEBEN@LEWISBRISBOIS.COM

July 25, 2014

Attorney General Joseph Foster
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Self Regional Healthcare — Notice of Data Security Event

Dear Sir:

We represent Self Regional Healthcare (“SRH”), 1325 Spring St, Greenwood, SC 29646, and are writing to notify you of a data event that may have compromised the security of two (2) New Hampshire residents’ protected health information. SRH’s investigation into this event is ongoing, and this notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, SRH does not waive any rights or defenses under New Hampshire law.

Nature of the Data Security Event

On or around May 25, 2014, two unauthorized individuals broke into one of Self Regional Healthcare’s facilities and stole a laptop belonging to a SRH employee. Upon learning of the burglary on May 27, 2014, SRH contacted law enforcement. SRH worked closely with law enforcement, and both intruders have been arrested. The thief responsible for stealing the laptop confessed to the crime. He stated that he never accessed the laptop, and that he destroyed and disposed of the laptop in a lake. The police sent divers in the water, but SRH and police have been unable to recover the laptop to date.

SRH takes the security of our patients’ personal information very seriously. SRH retained third-party forensic experts to assist with the investigation of this incident. At present, it appears possible that certain protected health information belonging to New Hampshire residents may have been accessible, including their name, Social Security number, treating physician name, insurance policy number, patient account number, service date, diagnosis/procedure information, financial account

July 25, 2014

Page 2

information, and address. We have received no reports of attempted or actual misuse of this information.

Notice to New Hampshire Residents

Although the investigations are ongoing, it appears that the protected information of two (2) New Hampshire residents may have been accessed without authorization as a result of this incident. SRH will send written notice of this incident to these two (2) residents on or about July 25, 2014, in substantially the same form as the letter attached here as *Exhibit A*.

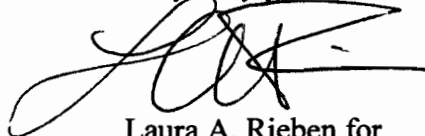
Other Steps Taken and To Be Taken

In addition to providing written notice of this incident to all affected individuals as described above, each affected individual is being offered access to one (1) free year of triple bureau credit monitoring services and identity restoration services. SRH is also providing each individual with information on how to protect against identity theft and fraud. SRH is providing written notice of this incident to the Department of Health and Human Services, to other state regulators as required, to the media, and to consumer reporting agencies.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at 215-977-4066.

Very truly yours,



Laura A. Rieben for
LEWIS BRISBOIS BISGAARD & SMITH LLP

LAR:sn
Enclosure

cc: Self Regional Healthcare

EXHIBIT A

[Date]

[Patient Name]

[Patient Address]

Dear [Patient]:

Self Regional Healthcare ("SRH") is writing to inform you of a recent incident that may affect the security of your protected health information. We are unaware of any attempted or actual misuse of your personal information, but are providing this notice to ensure that you are aware of the incident, so that you may take steps to protect your information should you feel it is appropriate to do so.

On May 27, 2014, we discovered that two unauthorized individuals broke into one of Self Regional Healthcare's facilities and stole a laptop belonging to a SRH employee. The theft occurred on Sunday, May 25, 2014. Upon learning of the burglary, SRH contacted law enforcement. SRH worked closely with law enforcement, and both intruders have been arrested. The thief responsible for stealing the laptop confessed to the crime and that he destroyed and disposed of the laptop in a lake. The police sent divers in the water, but SRH and police have been unable to recover the stolen hardware to date.

SRH takes the security of our patients' personal information very seriously. SRH retained third-party forensic experts to assist with the investigation of this incident, even though the intruders admitted their actions to law enforcement and claimed never to have accessed the laptop. Since the laptop has not been recovered, we are taking precautionary measures to let you know there is a possibility that someone may have accessed your protected health information, including your name, [Social Security number], [driver's license number], [treating physician name], [insurance policy number], [patient account number], [service date], [diagnosis/procedure information] [payment card information], [financial account information], and possibly your address.

In an abundance of caution, SRH is providing written notice of this incident to you, to the U.S. Department of Health and Human Services, as well as to certain state regulators. In order to help further safeguard you from any potential misuse of your personal information, we are offering you access to a **complimentary** one-year membership of Experian's[®] ProtectMyID[®] Alert. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

Activate ProtectMyID Now in Three Easy Steps:

1. **ENSURE That You Enroll By: October 31, 2014** (Your code will not work after this date.)
2. **VISIT the ProtectMyID Web Site to enroll: www.protectmyid.com/redeem**
3. **PROVIDE Your Activation Code: [code]**

If you have questions or need an alternative to enrolling online, please call 877-371-7902 and provide engagement #: [engagement number].

Additional details regarding your {12-MONTH} ProtectMyID Membership:

A credit card is not required for enrollment.

Once your ProtectMyID membership is activated, you will receive the following features:

- **Free copy of your Experian credit report**
- **Surveillance Alerts for:**
 - **Daily Bureau Credit Monitoring:** Alerts of key changes & suspicious activity found on your Experian, Equifax[®] and TransUnion[®] credit reports.
- **Identity Theft Resolution & ProtectMyID ExtendCARE:** Toll-free access to US-based customer care and a dedicated Identity Theft Resolution agent who will walk you through the process of fraud resolution from start to finish for seamless service. They will investigate each incident; help with contacting credit grantors to dispute

charges and close accounts including credit, debit and medical insurance cards; assist with freezing credit files; contact government agencies.

- It is recognized that identity theft can happen months and even years after a data breach. To offer added protection, you will receive ExtendCARE™, which provides you with the same high-level of Fraud Resolution support even after your ProtectMyID membership has expired.
- **\$1 Million Identity Theft Insurance***: Immediately covers certain costs including, lost wages, private investigator fees, and unauthorized electronic fund transfers.

Once your enrollment in ProtectMyID is complete, you should carefully review your credit report for inaccurate or suspicious items. If you have any questions about ProtectMyID, 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 877-371-7902.

We encourage you to remain vigilant, to review your account statements, and to monitor your credit reports and explanation of benefits forms 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.

At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

Equifax
P.O. Box 105069
Atlanta, GA 30348
800-525-6285
www.equifax.com

Experian
P.O. Box 2002
Allen, TX 75013
888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19022-2000
800-680-7289
www.transunion.com

You can also further educate yourself regarding identity theft, and the steps you can take to protect yourself, by contacting your state Attorney General or the Federal Trade Commission. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. Instances of known or suspected identity theft should be reported to law enforcement, your Attorney General, and the FTC. You can also further educate yourself about placing a fraud alert or security freeze on your credit file by contacting the FTC or your state's Attorney General. For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, (919) 716-6400, www.ncdoj.gov. For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, (888) 743-0023, www.oag.state.md.us.

Our patients' safety and privacy are our utmost priority and we deeply regret this has happened. We've established a confidential inquiry line, staffed with professionals trained in identity and credit protection and restoration, and familiar with this incident and the contents of this letter. This confidential inquiry line is available Monday through Friday, 9:00 a.m. to 7:00 p.m. E.S.T. at XXX-XXX-XXXX.

Sincerely,

James A. Pfeiffer
President & CEO

4841-9447-5804.1 * Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of AIG. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.