NOTICE OF DATA PRIVACY EVENT

ABOUT THE DATA PRIVACY EVENT

Beacon Health System ("Beacon") recently discovered an incident that may affect the security of personal information of about one hundred and fifty Beacon patients. We take this incident very seriously, and we have been working diligently, with the assistance of third-party forensic investigators, to determine the full nature and scope of this incident. We are taking additional actions to strengthen the security of our email systems moving forward. Beacon is also contacting the appropriate regulators regarding this incident.

What happened? On April 2, 2018, Beacon became aware of suspicious activity relating to an employee email account. We quickly launched an investigation to determine what may have happened and what information may have been affected. Working together with a leading computer forensics expert, our investigation determined that an unknown individual had access to the email account of a medical secretary for several hours on April 2, 2018. Because we were unable to determine which email messages may have been opened by the unauthorized individual, we reviewed the email account to identify what personal information was stored within it. We have no evidence that the personal information of Beacon patients was actually accessed, viewed, or acquired without permission. We are providing this notification out of an abundance of caution.

What information may have been affected by this incident? Recently, Beacon determined that the affected email account contained, and the unauthorized actor may have had access to, information related to certain Beacon patients, including the following types of information: name, date of birth, Social Security number, patient identification number, treatment information, treatment location, procedure information, physician's name, medical history, medical record number, mental or physical condition, diagnosis information, clinical information, telephone number, financial account number, credit or debit card number, health insurance information, subscriber member number, dates of treatment

The type of information affected varies per impacted individual. Social Security numbers were only impacted for some of the affected population. While our investigation is ongoing, we do not currently have any evidence of actual or attempted misuse of patient information as a result of this incident.

How will I know if I am affected by this incident? For individuals where address information is available, Beacon is mailing notice letters to the individuals whose protected information was contained within the affected email account and may have been accessed by an unauthorized actor. If you think you are affected but did not receive a letter, you should call the number provided below.

What is Beacon doing? Information privacy and security are among our highest priorities. Beacon has strict security measures to protect the information in our possession. Upon learning

of this incident, we quickly took steps to assess our security systems, disabled the impacted employee email account, changed the password, and notified our other employees to be on the lookout for suspicious emails. We are currently implementing additional training and education for employees to prevent similar future incidents. Although we are not aware of any actual or attempted misuse of our patients' information, we are also providing the impacted individuals access to complimentary credit monitoring services as an added precaution.

Whom should I contact for more information? We recognize that you may have questions not addressed in this notice. If you have additional questions, please call our dedicated assistance line at 855-255-4850 (toll free), Monday through Friday, 9:00 a.m. to 9:00 p.m., EST.

What can I do to protect my information?

Monitor Your Accounts.

Credit Reports. Beacon encourages potentially impacted individuals to remain vigilant against incidents of identity theft and fraud, to review account statements, and to monitor their 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.

Fraud Alerts. 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	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
1-800-525-6285	1-888-397-3742	1-800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

Security Freeze. You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on

your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. If you have been a victim of identity theft and you provide the credit bureau with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. Fees vary based on where you live, but commonly range from $3 to $15. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. In order to request a security freeze, you will need to supply your full name, address, date of birth, Social Security number, current address, all addresses for up to five previous years, email address, a copy of your state identification card or driver's license, and a copy of a utility bill, bank or insurance statement, or other statement proving residence.

Indiana residents can request a credit freeze free of charge. There is no fee for Indiana residents to place, temporarily lift, remove, or request a new password or PIN.

To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze	Experian Security Freeze	TransUnion
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
1-800-685-1111	1-888-397-3742	1-888-909-8872
https://www.freeze.equifax.com	www.experian.com/freeze/	www.transunion.com/

Additional Information.
You can 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/idtheft; 1-877-ID-THEFT (1-877-438-4338); and 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.