Seven Counties Services

December 21, 2024

Dear CLIENT NAME:

We are writing to tell you about an electronic data security incident that occurred at Seven Counties Services, Inc. from July 19, 2024 to August 12, 2024, that may have compromised your protected health information. Data that included your personal information was compromised. We are contacting you directly to explain the circumstances of the incident and to advise you of steps you can take to protect your personal information.

**What happened?**
The incident is believed to have begun on July 19, 2024 as the result of a phishing email that sent emails to other staff that appeared to be from a trusted source. Staff responded to the request and their email accounts were compromised. The incident was discovered by our IT Department on August 12, 2024 and the accounts were immediately secured. The electronic health record system was not accessed or compromised. The nature and scope of the incident required time to analyze, and we have determined that your information may have been impacted.

**What information was involved?**
Our organization maintains demographic, financial and clinical protected health information about you in order to provide services. This information, which is primarily stored electronically, can be shared internally with staff by email messages and reports on a need-to-know basis. Reports contain names and several reports contain the following: date of birth, social security number, address, phone number, email, driver's license number, diagnosis information, diagnosis code, medical history /condition /treatment /prescription Information, individual tax identification number, medical record number, other government ID number, health insurance individual policy number, Medicare/Medicaid numbers, patient account number, date of service, certificate license numbers, and full face photo. Any email that contained information about you or a document or report as an attachment, could have been compromised.

**What additional action did Seven Counties Services take in response to the incident?**
To reduce a future reoccurrence of a similar incident and to better protect the organization, our IT Department is investigating up better access controls. The organization had already implemented a flag on emails received from outside our organization by adding an External Email banner to such emails. This External Email banner is intended to aide employees in identifying email from someone posing to be from a trusted source from within our organization as well as other suspicious emails. Since this incident, the IT department has posted more educational information for employees regarding phishing attacks and spoofing email and how to be vigilant against these types of malicious emails.

**What should I do now?**
While banking information was likely not exposed, it is prudent to review account transactions regularly and to closely monitor all financial accounts, including credit cards, checking and saving accounts, 401k etc. We encourage you to monitor your credit regularly. You should look out for new accounts that may have been



Corporate Office
10401 Linn Station Road, Suite 100
Louisville, KY 40223
sevencounties.org

established in your name but not by you. Below are the three main credit reporting agencies, as well as free resources, to help you monitor your credit or to repot identity theft.

| Equifax | Experian | TransUnion |
|---|---|---|
| PO Box 105788 | P.O. Box 9554 | PO Box 2000 |
| Atlanta, GA 30348 | Allen, TX 75013 | Fullerton, CA 92834-6790 |
| (800) 525-6285 | (888)397-3742 | (800) 680-7289 |
| www.equifax.com | www.experian.com | www.transunion.com: |

You also can order a free copy of your credit report once every 12 months by visiting www.annualcreditreport.com, which is also available from the FTC website with additional information https://www/ftc/gov/faq/consumer-protection/get-my-free-credit-report. You may also contact the FTC for information on how to prevent or avoid identity theft: http://www.identitytheft.gov/infor-lost- or-stolen.

If you believe you have been a victim of identity theft related to the incident described here since July 19, 2024, or have reason to believe that your information has been misused, you should immediately contact the U.S. Federal Trade Commission (FT) and/or the consumer protection agencies.

- **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idteft/, 1-877IDTHEFT (438-4338).
- **Kentucky: Office of Consumer Protection**, 1024 Capital Center Drive, Suite 200, Frankfort, Kentucky 40601, Phone (502) 696-5389; **Identify Theft Hotline**: (888) 432-9257

If you have questions or concerns, you may contact me at the following number, 1-888-580-1002, Monday through Friday, 8:30 am – 4 pm or by e-mail at SCSfeedback@sevencounties.org.

Sincerely,

Barbara Orr, RHIA

Barbara Orr
Health Information Officer