Kim Detwiler, Partner
Cybersecurity & Data Privacy Team
1650 Market Street, Suite 3600
Philadelphia, PA 19103
kdetwiler@constangy.com
Mobile: 484.999.1307

Emergency: BreachResponse@constangy.com
Hotline: 877-382-2724 (877-DTA-BRCH)

June 1, 2026

VIA ONLINE SUBMISSION
Attorney General Aaron Frey
Office of the Attorney General
Consumer Protection Division
Security Breach Notification
111 Sewall Street, 6th Floor
Augusta, ME 04330

Re: Notice of Data Event

To Whom It May Concern:

We represent Clarinda Regional Health Center ("Clarinda"), located at 220 Essie Davison Drive, Clarinda, Iowa 51632, and are writing to notify your office of an incident that may affect the security of certain personal information relating to 1 resident. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Clarinda does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

1. Nature of the Security Incident

On December 15, 2025, Clarinda discovered suspicious activity within its network environment. Clarinda promptly initiated an investigation of the matter and engaged cybersecurity experts to assist with the process. As a result of the investigation, Clarinda determined that certain files may have been acquired without authorization in or around October 2025. Clarinda undertook a comprehensive review of those files and learned that certain personal information was contained within the potentially affected data. Clarinda then gathered the information needed to effectuate notice, including but not limited to the names of the affected individuals and their address information, which was completed on May 21, 2026.

The information that could have been subject to unauthorized access includes first and last name, as well as Social Security number.

2. Notice to Maine Residents

On or about June 1, 2026, Clarinda provided written notice of this incident to approximately 1 resident. Written notice is being provided in substantially the same form as the letter attached here as **Exhibit A**.

3. Other Steps Taken and to Be Taken

Upon discovering the event, Clarinda moved quickly to investigate and respond to the incident, assess the security of its network, and identify potentially affected individuals. For individuals with exposed Social Security numbers, Clarinda is providing access to credit monitoring services for 12 months through TransUnion to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Clarinda is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Clarinda is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

4. Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact me at 484.999.1307.

Very truly yours,

Kim Detwiler

Kim Detwiler of
Constangy, Brooks, Smith & Prophete LLP

0000424

Clarinda Regional Health Center
c/o Cyberscout
555 Monster Rd SW
Renton, WA 98057
USBFS3729

3_0000424

NAME
ADDRESS

June 1, 2026

Subject: Notice of Data Security Incident

Dear NAME:

We are writing to inform you of a recent data security incident experienced by Clarinda Regional Health Center ("Clarinda") that may have involved your personal information. Please read this letter carefully as it contains information regarding the incident and steps that you can take to help protect your information.

What Happened. On or around December 15, 2025, we learned that certain data within our network may have been accessed without authorization. In response, we promptly initiated an investigation and engaged cybersecurity experts to assist with the process. The investigation revealed that certain files may have been acquired by an unauthorized actor in or around October 2025. After the investigation concluded, we undertook a comprehensive review of the relevant files with the assistance of a third-party vendor and determined that personal information was involved. We then worked to secure the information needed to effectuate notice, including address information, for the impacted individuals. This process was completed on May 21, 2026.

What Information Was Involved. The information may have included your name as well as your [EXPOSED DATA ELEMENTS].

What We Are Doing. In response to the incident, we took the steps described above and implemented measures to enhance security and minimize the risk of a similar incident occurring in the future. We are also providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for 12 months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

What You Can Do: To enroll in Credit Monitoring services at no charge, please log on to https://bfs.cyberscout.com/activate and follow the instructions provided. When prompted, please provide the following unique code to receive services: INSERT CODE. In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of

age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

For More Information. Further information about how to protect your personal information appears on the following page. If you have questions or need assistance, please call 1-833-289-3437 between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays

We take your trust in us and this matter very seriously and regret any inconvenience this may cause.

Sincerely,

Clarinda Regional Health Center
220 Essie Davison Drive
Clarinda, IA 51632

0000424

Steps You Can Take to Help Protect Your Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (the "FTC").

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting www.annualcreditreport.com, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax
P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian
P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at www.annualcreditreport.com.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov
877-438-4338

California Attorney General
1300 I Street
Sacramento, CA 95814
www.oag.ca.gov/privacy
800-952-5225

Iowa Attorney General
1305 E. Walnut Street
Des Moines, Iowa 50319
www.iowaattorneygeneral.gov
888-777-4590

Kentucky Attorney General
700 Capitol Avenue, Suite 118
Frankfort, Kentucky 40601
www.ag.ky.gov
502-696-5300

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
www.marylandattorneygeneral.gov/Pages/CPD
888-743-0023

New York Attorney General
The Capitol
Albany, NY 12224
ag.ny.gov
800-771-7755

NY Bureau of Internet and Technology
28 Liberty Street
New York, NY 10005
www.dos.ny.gov/consumerprotection/
212.416.8433

NC Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov/protectingconsumers/
877-566-7226

Oregon Attorney General
1162 Court St., NE
Salem, OR 97301
www.doj.state.or.us/consumer-protection
877-877-9392

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
www.riag.ri.gov
401-274-4400

Washington D.C. Attorney General
400 S 6th Street, NW
Washington, DC 20001
oag.dc.gov/consumer-protection
202-442-9828

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.