October 2, 2026

CONFIDENTIAL – INTENDED FOR RECIPIENTS ONLY

SENT VIA EMAIL:

Re: Notice of Data Breach

To Whom It May Concern:

Telecare writes to provide you with notice of an incident that may have exposed the personal information of persons served associated with your practice. This letter provides you with information about what happened, what we've done in response, and what steps are available to you.

What Happened?

On or around January 25, 2026, Telecare discovered unusual activity involving its digital environment. Telecare promptly responded and launched an investigation to confirm the nature and scope of the incident with the assistance of third-party cybersecurity experts. The investigation revealed that the incident impacted certain data. Following this determination, we engaged a data mining vendor to conduct extensive electronic discovery to determine the specific information impacted, and to whom that information pertained. That process was completed on September 4, 2026, and you are being notified based on the results of this discovery.

What Information Was Involved?

The affected information includes protected health information of certain individuals affiliated with your organization. We have found no evidence that information has been misused. However, the information involved for persons served may include name, address, Social Security number, date of birth, driver's license number, diagnoses/conditions, treatment information, lab results, medications, medical record or patient ID number, and health insurance information exposure for certain patients as a result of this incident. **Notably, the types of information affected were different for each individual, and not every individual had all the above listed elements exposed.**

The list of affected individuals and specific data elements involved for each person will be provided to your organization upon request *(see Next Steps below)*.

What We Are Doing.

As part of our investigation, we worked with cybersecurity professionals to secure our network. We have reset credentials, enhanced our security measures and monitoring tools, and are reviewing our existing policies and training protocols to help prevent similar incidents in the future. This was an isolated incident, operations were not materially impacted, and we are taking all necessary actions to address the situation and reduce risk going forward.

Next Steps and Services We are Offering.

1. **Obtain Your Data File of Affected Individuals**

Please send an **email** to **TelecareIncident@lewisbrisbois.com** by **October 7, 2026**, and we will make arrangements to securely transfer a data file with the list of individuals related to your organization whose protected health information was impacted by this incident.

2. **Opt-Out**

Under applicable law, your practice may be required to provide notice of this event to the potentially affected individuals as well as certain regulators. We are unable to provide you with legal advice on this issue and recommend you discuss the contents of this letter and your organization's potential notification duties with legal counsel should you require specific legal guidance.

Telecare is offering to notify all affected individuals, HHS OCR, and state regulators on your behalf. Enclosed with this correspondence is a sample notification letter. **Please note that outside of variable elements, Telecare cannot make any changes to the individual notification letters.**

If you do **not** want Telecare to provide notice on your behalf, please **email TelecareIncident@lewisbrisbois.com** on or before **October 12, 2026**, to indicate that you OPT-OUT to Telecare notifying impacted individuals on your behalf.

Unless we receive notice from you electing to opt out, Telecare will provide written notice of this event to individuals on behalf of your practice and will notify HHS OCR and state regulators.

If you elect to OPT-OUT, Telecare will **not** provide notice on your behalf.

3. **Website and Media Notification**

Telecare has posted notice to its website. Telecare is also going to send nationwide media notices. An example of the **media notification** is included.

***

We sincerely apologize for any worry or inconvenience this incident may cause. We appreciate your patience and understanding throughout this incident. If you have questions, please contact **TelecareIncident@lewisbrisbois.com.**

Encls:
Sample Individual Notification Letter
Sample Regulatory Notification Letter
Media Notification

Telecare Corporation

<<Return Address>>
<<City>>, <<State>> <<Zip>>

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

Enrollment Code: <<XXXXXXXX>>
Enrollment Deadline: <<Date>>

To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
[IDX URL]

<<Date>>

Subject: Notice of <<Custom Field 1>>

Dear <<FIRSTNAME>> <<LASTNAME>>:

We are writing to notify you of a data security incident that involved your information. Telecare received your information in connection with health services Telecare performed for you on behalf of <<Data Owner>>. While we are unaware of any attempted or actual misuse of your information at this time, this notice provides you with information about the incident, our response, and resources available to help protect your information.

What Happened?

On or around January 25, 2026, Telecare discovered unusual activity involving its digital environment. We promptly responded and launched an investigation to confirm the nature and scope of the incident with the assistance of third-party cybersecurity experts. After extensive electronic discovery, which was completed on September 4, 2026, it was determined that your personal information was present in the impacted data set. We immediately took steps to notify you as soon as the investigation was completed.

What Information Was Involved?

The potentially impacted information may include your name and the following: <<Exposed Data Elements>>.

What Are We Doing?

As soon as we discovered the incident, we moved quickly to initiate a response, which included conducting a thorough investigation with the assistance of cybersecurity specialists and confirming the security of our network environment. We are continually reviewing and revising technical safeguards and making enhancements to reduce the likelihood of a similar event in the future.

[redacted]

In addition, although we have no evidence that your information has been misused, we are offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: [12 months/24 months] of credit monitoring, CyberScan monitoring and fully managed ID theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What Can You Do?

To enroll in identity protection services at no charge, please visit [IDX URL] or scan the QR image and use the Enrollment Code provided above.

We encourage you to take full advantage of this service offering. Enclosed you will find additional materials regarding the resources available to you, and the steps you can take to further protect your personal information.

For More Information.

Representatives are aware of the incident and can answer questions or concerns you may have regarding protection of your personal information. Please call <<CALL CENTER NUMBER>>, Monday through Friday, 8:00 A.M. to 8:00 P.M. ET, excluding holidays, for assistance or for any additional questions you may have.

Additional Information

Credit Reports: You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number;
(3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles.

The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion Security Freeze**
P.O. Box 105788 Atlanta, GA 30348 1-888-298-0045 https://www.equifax.com/personal/credit-report-services/credit-freeze/	P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html	P.O. Box 160 Woodlyn, PA 19094 1-800-916-8800 www.transunion.com/credit-freeze

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with:

- Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf);
- TransUnion (https://www.transunion.com/fraud-alerts); or
- Experian (https://www.experian.com/fraud/center.html).

A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are listed above.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

File Police Report: You have the right to file or obtain a police report if you experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

FTC and Attorneys General: 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. This notice has not been delayed by law enforcement.

For Arizona residents, the Attorney General may be contacted at the Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004, 1-602-542-5025.

For Colorado residents, the Attorney General may be contacted through Consumer Protection 1300 Broadway, 9th Floor, Denver, CO 80203 1-720-508-6000, www.coag.gov.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and oag.dc.gov.

For Illinois residents, the Attorney General can be contacted at 100 West Randolph Street**,** Chicago, IL 60601**;** 1-866-999-5630**;** www.illinoisattorneygeneral.gov.

For Iowa residents, you can report any suspected identity theft to law enforcement or to the Attorney General.

For Massachusetts residents, it is required by state law that you are informed of your right to obtain a police report in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For Maryland residents, the Maryland Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, and www.oag.state.md.us. Telecare's address is 1080 Marina Village Parkway, Suite 100, Alameda, CA 94501.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the Attorney General may be contacted at Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, and https://ag.ny.gov/.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General can be reached at 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed regarding this incident. There are approximately [#] Rhode Island residents that may be impacted by this event.

For Vermont Residents: If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).

October 2, 2026

NAME
ADDRESS 1
ADDRESS 2
CITY, STATE ZIP

Email: EMAIL

Re: Notification of Data [Security Incident / Breach]

Dear NAME:

Lewis Brisbois represents Telecare Corporation, headquartered in Alameda, California, in connection with a recent data security incident described in greater detail below. The purpose of this letter is to notify you of the incident in accordance with [STATE] data breach notification law.

1. Nature of the [Security Incident / Breach]

On or around January 25, 2026, Telecare discovered suspicious activity related to its digital environment. Telecare promptly responded and launched an investigation to confirm the nature and scope of the incident with the assistance of third-party cybersecurity experts. The investigation revealed that certain data was impacted by the incident. Following this determination, an in-depth and comprehensive review of potentially impacted data was conducted to determine what information was compromised, and to whom it pertained. That process was completed on September 4, 2026.

2. Type of Information and Number of [STATE] Residents Affected

Telecare notified [NUMBER] residents of [STATE] of this data [security incident / breach] via first class U.S. mail on [MAILING DATE]. The information accessed and potentially acquired by the unauthorized actor responsible for this incident may have included name, address, Social Security number, date of birth, driver's license number, diagnoses/conditions, treatment information, lab results, medications, medical record or patient ID number, and health insurance information exposure for certain persons served as a result of this incident. **Notably, the types of information affected were different for each individual, and not every individual had all the above listed elements exposed.**

A sample copy of the notification letter sent to the impacted individuals is included with this correspondence.

3. Additional Steps Taken Relating to the Incident

Telecare implemented additional security features in an effort to prevent a similar incident from occurring in the future. Further, Telecare has offered [twenty-four (24) / twelve (12)] months of complimentary services through TransUnion, which includes credit monitoring, cyber monitoring, identity theft restoration services, an insurance reimbursement policy, and access to a call center.

4. Contact Information

Telecare remains dedicated to protecting the personal information in its possession. If you have any questions or need additional information, please do not hesitate to contact me at my office number, XXX-XX-XXXX, or by email at XXXXX@XXXX.com.

Encl.: Sample Consumer Notification Letter

Notice of Data Security Incident

Alameda, California – October XX, 2026 – Telecare Corporation ("Telecare") is notifying individuals whose personal information may have been involved in a network security incident. This statement is intended to notify potentially impacted individuals about the incident, steps Telecare has taken in response, and resources available to assist and protect individuals.

What Happened? On or around January 25, 2026, Telecare discovered unusual activity within its digital environment. Upon discovery of this activity, Telecare took measures to secure the network and engaged a team of cybersecurity experts to assess, contain, and remediate the incident. The investigation determined that certain data may have been acquired without authorization as a result of the incident. After a thorough review of the impacted data, which was completed on September 4, 2026, it was determined that certain personal information may have been impacted. **Telecare has no evidence of misuse, or attempted misuse, of any potentially affected information.**

What Information Was Involved? Telecare's investigation identified instances of name, address, Social Security number, date of birth, driver's license number, diagnoses/conditions, treatment information, lab results, medications, medical record or patient ID number, and health insurance information exposure for certain persons served as a result of this incident. **Notably, the types of information affected were different for each individual, and not every individual had all the above listed elements exposed.**

What Are We Doing? Telecare takes its responsibility to safeguard information seriously and regrets any concern this incident may have caused. Upon detecting this incident, Telecare moved quickly to initiate a response, which included conducting a thorough investigation with the assistance of cybersecurity specialists and confirming the security of its network environment. Telecare took steps and is continually reviewing and revising technical safeguards and making enhancements to reduce the likelihood of a similar event in the future. Additionally, Telecare is committed to helping those people who may have been impacted by this situation.

The notification letter to the potentially impacted individuals includes steps that they can take to protect their information. In order to address any concerns and mitigate any exposure or risk of harm following this incident, Telecare has arranged for complimentary credit monitoring services and identity theft protection services to all potentially impacted individuals at no cost to them for a period of twelve months. Telecare recommends that individuals enroll in the services provided and follow the recommendations contained within the notification letter to ensure their information is protected.

For More Information. Individuals seeking more information or with questions about this incident may contact the dedicated call center at <<CALL CENTER NUMBER>> from 8:00 A.M. to 8:00 P.M. ET, Monday through Friday, excluding holidays.

Telecare sincerely regrets any inconvenience or concern that this matter may cause.