[redacted]

P
[redacted]

[redacted]

000010103G0500

P

NOTICE OF DATA BREACH

Re: **Important Security Notification**
Please read this letter.

Dear [redacted],

On behalf of the group health plans of Stanford and its affiliated health care entities ("Stanford"), Brightline is writing to inform you about a data security incident involving Fortra (formerly known as HelpSystems), a third-party provider of file transfer services known as GoAnywhere MFT Software-as-a-Service ("SaaS"), that affected some of your personal information (see "What Information Was Involved," below). We understand that the GoAnywhere MFT security incident affected multiple organizations and businesses, including those in the medical sector.

We value your relationship and respect the privacy of your personal information. We want you to understand the steps we have taken to address this issue and additional steps you can take to protect your personal information. The remaining sections of this letter explain the incident and offer you additional assistance for protecting your information, including complimentary identity theft protection and credit monitoring services.

What Happened: While Fortra's investigation is ongoing, we understand that on January 30, 2023, Fortra was made aware of suspicious activity within certain instances of its GoAnywhere MFT SaaS. Through its investigation, Fortra states that it identified a previously-unknown vulnerability which an unauthorized party used to access certain GoAnywhere customers' accounts and download files.

Fortra informed customers, including Brightline, about the security vulnerability in their GoAnywhere MFT SaaS on February 4, 2023. We took swift action the same day in response to the notice by confirming Fortra deactivated the unauthorized user's credentials, disabled the vulnerable java servlet, and rebuilt Brightline's instance on new infrastructure. Further, we implemented additional security measures, including a whitelisting for limited IP addresses to access the previously vulnerable administrative portal, removal of all Brightline data from the GoAnywhere MFT SaaS, and ongoing measures to reduce data exposure until an alternative file transfer solution is identified and implemented. Additionally, we retained cyber counsel to assist with our investigation. Our investigation determined the incident was limited solely to the GoAnywhere MFT SaaS. Fortra also promptly notified law enforcement and we understand it is cooperating with their investigation of the GoAnywhere incident.

Subsequently, we determined that the unauthorized party acquired certain files that were saved in the GoAnywhere MFT SaaS. After making this determination, we immediately began to analyze the files to determine which individuals and data had been affected. As part of that analysis, we have determined that those files contained some of your personal information, which is why we sent you this notice and are providing the services outlined in this letter.

What Information Was Involved: Based on the investigation, we identified some of your personal information in the files that the unauthorized party acquired through the GoAnywhere MFT SaaS, potentially including some combination of the following data elements: your name, your address, your member ID, your date of birth, your phone number, your employer's name and their group ID number, and your coverage start/end dates. The group health plans' files were shared with Brightline for verification of eligibility under the plans as well as potential outreach to plan participants who could benefit from Brightline's services.

What We Are Doing: As soon as we became aware of the incident, we took immediate action to investigate it, including confirming Fortra deactivated the unauthorized user's credentials, disabled the vulnerable java servlet, and rebuilt Brightline's instance on new infrastructure. Further, we implemented additional security measures, including a whitelisting for limited IP addresses to access the previously vulnerable administrative portal, removal of all Brightline data from the GoAnywhere MFT SaaS, and ongoing measures to reduce data exposure until an alternative file transfer solution is identified and implemented. We retained cyber counsel to assist with our investigation, and we understand that Fortra notified law enforcement. While our investigation has determined that the incident is limited to the GoAnywhere MFT SaaS, we continue to enhance our cybersecurity program to further safeguard our systems from cyber threats.

As a precaution, we have secured the services of Cyberscout to provide identity theft restoration and credit monitoring services at no cost to you for **2 years.**

In response to the incident, we are 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 2 years 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 through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

How To Enroll For Free Services: To enroll in Credit Monitoring services at no charge, please log on to [redacted] and follow the instructions provided. When prompted please provide the following unique code to receive services: [redacted]. 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.

What You Can Do:

Order Your Free Credit Report. To order your free annual credit report, visit www.annualcreditreport.com, call toll-free at (877) 322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's (FTC) website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

The three credit bureaus (Equifax, Experian, and TransUnion) provide free annual credit reports only through the website, toll-free number, or request form. You may also purchase a copy of your credit report by contacting any of the credit reporting agencies below:

Equifax www.equifax.com	(800) 685-1111
Experian www.experian.com	(888) 397-3742
TransUnion www.transunion.com	(800) 916-8800

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Upon receiving your credit report, review it carefully. Errors may be a warning sign of possible identity theft. Here are a few tips of what to look for:

- Look for accounts you did not open.
- Look in the "inquiries" section for names of creditors from whom you have not requested credit. Some companies bill under names other than their store or commercial names; the credit bureau will be able to tell if this is the case.
- Look in the "personal information" section for any inaccuracies in information (such as home address and Social Security Number).

If you see anything you do not understand, call the credit bureau at the telephone number on the report. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing. Information that cannot be explained should also be reported to your local police or sheriff's office because it may signal criminal activity.

We encourage you to take advantage of these protections and remain vigilant for incidents of fraud and identity theft, including regularly reviewing and monitoring your credit reports and account statements.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state, and local law enforcement. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft.
You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).
For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.
For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226 for more information about preventing identity theft.
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; https://ag.ny.gov/.
For Connecticut residents: You may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.
For Massachusetts residents: You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html.
For Rhode Island residents: You may contact the Office of the Attorney General, 150 South Main Street, Providence, RI 02903, (401) 274-4400, https://riag.ri.gov/.

Reporting of identity theft and obtaining a police report.
For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.
For Massachusetts residents: You have the right to obtain a police report.
For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.
For Rhode Island residents: You have the right to obtain a police report.

Placing a Security Freeze. You have a right to place a "security freeze" on your credit report, at no charge, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit.

You can place, temporarily lift, or permanently remove a security freeze on your credit report online, by phone, or by mail. You will need to provide certain personal information, such as address, date of birth, and Social Security number to request a security freeze and may be provided with a unique personal identification number (PIN) or password, or both, that can be used by you to authorize the removal or lifting of the security freeze. Information on how to place a security freeze with the credit reporting agencies is also contained in the links below:

https://www.equifax.com/personal/credit-report-services/
https://www.experian.com/freeze/center.html
https://www.transunion.com/credit-freeze

As of February 20, 2023, the reporting agencies allow you to place a credit freeze through the online, physical mail and phone numbers and request that you provide the information listed below. Where possible, please consult the websites listed above for the most up-to-date instructions.

Reporting Agency	**Online**	**Physical Mail**	**Phone Number**
Equifax	***Freeze request may be submitted via your myEquifax account, which you can create here:*** https://my.equifax.com/consumer-registration/UCSC/#/personal-info	***Mail the Equifax Freeze Request Form to:*** Equifax Information Services LLC P.O. Box 105788 Atlanta, GA 30348-5788 ***Form may be found here:*** https://assets.equifax.com/assets/personal/Security_Freeze_Request_Form.pdf	888-298-0045
Experian	***Freeze request may be submitted here:*** https://www.experian.com/ncaconline/freeze	***Mail the request to:*** Experian Security Freeze, P.O. Box 9554, Allen, TX 75013 ***Request must include:*** • Full Name • Social security number • Complete address for last 2 years • Date of birth • One copy of a government issued identification card, such as a driver's license, state ID card, etc. • One copy of a utility bill, bank or insurance statement, etc.	888-397-3742

TransUnion	***Freeze request may be submitted via your TransUnion account, which you can create here:*** https://service.transunion.com/dss/orderStep1_form.page?	***Mail the request to:*** TransUnion P.O. Box 160 Woodlyn, PA 19094 ***Request must include:*** • Full Name • Social security number • Complete address	888-909-8872

Fees associated with placing, temporarily lifting, or permanently removing a security freeze no longer apply at nationwide consumer reporting agencies.

Placing a Fraud Alert. To protect yourself from possible identity theft, you have the right to place an initial or extended fraud alert on your credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. You may obtain additional information from the FTC and the credit reporting agencies listed above about placing a fraud alert and/or security freeze on your credit report.

More Information: Brightline is committed to data protection. We regularly review our physical and electronic safeguards to protect personal information, and we will continue to take appropriate steps to safeguard personal information and our systems. On behalf of Stanford, we deeply regret any inconvenience or concern this may have caused. Should you have any additional questions, you may contact us at [redacted] from 8:00 am to 8:00 pm Eastern time, Monday through Friday, excluding holidays.

Sincerely,
Brightline