Thank you for using version 2025.4.1104.462 of Telerik Document Processing Libraries. Access to the latest updates and support requires a valid license. Renew your license and download a new license key. Learn more about Telerik Document Processing Libraries licensing https://prgress.co/3PwQMut

Lauren Godfrey, Partner
322 North Shore Drive
Building 1B, Suite 200
Pittsburgh, Pennsylvania 15212
412-870-4129

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

November 9, 2026

VIA ELECTRONIC MAIL
Attorney General Nick Brown
Office of the Attorney General
Consumer Protection Division
1125 Washington Street SE
P.O. Box 40100
Olympia, WA 98504-0100

Re: Supplemental Notification of Data Security Incident

To Whom It May Concern:

Constangy, Brooks, Smith & Prophete, LLP represents Dorsata, Inc., located at 240 W Main St., Suite 100-V62, Charlottesville, VA 22902-5009, in connection with its response to a recent data security incident discussed below. The purpose of this letter is to supplement **Report Number: A43427** submitted on October 21, 2026, in accordance with the Washington data breach notification statute. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Dorsata, Inc. does not waive any rights or defenses regarding the applicability of Washington law, the applicability of the Washington data security incident notification statute, or personal jurisdiction.

1. Nature of the Security Incident

Dorsata, Inc. partners with women's health clinics and physicians to provide certain technology that is used in conjunction with healthcare provider's electronic health records system.

On August 12, 2026, Dorsata received a notice that the Metabase business intelligence software it uses contained a security vulnerability. Dorsata immediately patched the software and began an investigation with the assistance of third-party cybersecurity experts. The investigation determined the Metabase security vulnerability allowed unauthorized access to our database platform from August 10, 2026, to August 12, 2026. Dorsata reviewed the data involved in the incident and advised healthcare provider partners that protected health information was contained within the affected data. Dorsata, Inc. worked diligently to identify the individuals to whom that personal information related and to provide notification of the Incident to them on behalf of the healthcare partners.

2. Number of Affected Washington Residents & Information Involved

Thank you for using version 2025.4.1104.462 of Telerik Document Processing Libraries. Access to the latest updates and support requires a valid license. Renew your license and download a new license key. Learn more about Telerik Document Processing Libraries licensing https://prgress.co/3PwQMut

The incident involved personal information for approximately 1,720 additional Washington residents. The information involved in the incident for identified Washington residents included name, date of birth, provider name, medical history, treatment location, medical insurance information, patient ID, and vaccines.

3. Notification to Identified Individuals

Between October 20, 2026 and October 21, 2026, Dorsata, Inc. issued notice to approximately 1,993 Washington residents. Between November 6, 2026 and November 9, 2026, notification letters issued to an additional 1,720 identified Washington residents by USPS First Class Mail. The notification letter provides resources and steps individuals can take to help protect their information.

4. Measures Taken to Address the Incident

Upon identifying this incident, in addition to taking the steps described above, Dorsata, Inc. worked to learn more about what happened and what information could have been affected. Dorsata, Inc. notified the identified individuals and provided them with steps they can take to protect their personal information, including providing them with information about its toll-free call center established to answer questions about the incident and address related concerns.

5. Contact Information

If you have any questions or need additional information regarding this event, please do not hesitate to contact me at lgodfrey@constangy.com.

Sincerely,

Lauren D. Godfrey

Lauren D. Godfrey
Partner, Constangy, Brooks, Smith & Prophete LLP

Thank you for using version 2025.4.1104.462 of Telerik Document Processing Libraries. Access to the latest updates and support requires a valid license. Renew your license and download a new license key. Learn more about Telerik Document Processing Libraries licensing https://prgress.co/3PwQMut

Dorsata, Inc.
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998



[redacted]

[redacted]

Subject: Notice of Data [redacted]

Dear [redacted]:

We are writing to inform you of a recent data security incident involving a third-party software vendor, Metabase, that may have affected your protected health information. Dorsata, Inc. partners with women's health clinics and physicians to provide certain technology that is used in conjunction with your healthcare provider's electronic health records system. 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 August 12, 2026, we received a notice that the Metabase business intelligence software we use contained a security vulnerability. We immediately patched the software and began an investigation with the assistance of third-party cybersecurity experts. Our investigation determined the Metabase security vulnerability allowed unauthorized access to our database platform from August 10, 2026, to August 12, 2026. We reviewed the data involved in the incident and advised your healthcare provider that your protected health information was contained within the affected data. Your healthcare provider then requested that we notify you of the incident, which is the reason for this notification. Please note that we have no evidence of the misuse, or attempted misuse, of any potentially impacted information.

What Information Was Involved. The information may have included your name, [redacted]. Your social security number was not involved.

What We Are Doing. As soon as we discovered this 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.

What You Can Do. You can follow the recommendations on the following page to help protect your information.

Thank you for using version 2025.4.1104.462 of Telerik Document Processing Libraries. Access to the latest updates and support requires a valid license. Renew your license and download a new license key. Learn more about Telerik Document Processing Libraries licensing https://prgress.co/3PwQMut

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 1-800-655-5832 Monday through Friday from 8:00 am to 8:00 pm ET, excluding holidays. We take your trust in us and this matter very seriously. Please accept our sincere apologies for any worry or inconvenience this may cause.

Sincerely,

Dorsata, Inc.
240 W Main St.
Suite 100-V62
Charlottesville, VA 22902-5009

Draft

Thank you for using version 2025.4.1104.462 of Telerik Document Processing Libraries. Access to the latest updates and support requires a valid license. Renew your license and download a new license key. Learn more about Telerik Document Processing Libraries licensing https://prgress.co/3PwQMut

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	**Experian**	TransUnion
P.O. Box 105851	P.O. Box 9532	1510 Chester Pike
Atlanta, GA 30348	Allen, TX 75013	Crum Lynne, PA 19022
1-800-525-6285	1-888-397-3742	1-800-916-8800
www.equifax.com	www.experian.com	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	**Maryland Attorney General**	**Oregon Attorney General**
600 Pennsylvania Ave, NW	200 St. Paul Place	1162 Court St., NE
Washington, DC 20580	Baltimore, MD 21202	Salem, OR 97301
consumer.ftc.gov	https://oag.maryland.gov	www.doj.state.or.us/consumer-protection
877-438-4338	888-743-0023	877-877-9392
California Attorney General	**New York Attorney General**	**Rhode Island Attorney General**
1300 I Street	The Capitol	150 South Main Street
Sacramento, CA 95814	Albany, NY 12224	Providence, RI 02903
www.oag.ca.gov/privacy	800-771-7755	www.riag.ri.gov
800-952-5225	ag.ny.gov	401-274-4400
Iowa Attorney General	**NY Bureau of Internet and Technology**	**Washington D.C. Attorney General**
1305 E. Walnut Street	28 Liberty Street	400 S 6th Street, NW
Des Moines, Iowa 50319	New York, NY 10005	Washington, DC 20001
www.iowaattorneygeneral.gov	www.dos.ny.gov/consumerprotection/	oag.dc.gov/consumer-protection
888-777-4590	212.416.8433	202-442-9828

Thank you for using version 2025.4.1104.462 of Telerik Document Processing Libraries. Access to the latest updates and support requires a valid license. Renew your license and download a new license key. Learn more about Telerik Document Processing Libraries licensing https://prgress.co/3PwQMut

Kentucky Attorney General 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601 www.ag.ky.gov 502-696-5300	**NC Attorney General** 9001 Mail Service Center Raleigh, NC 27699 ncdoj.gov/protectingconsumers/ 877-566-7226	

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.

Draft

Thank you for using version 2025.4.1104.462 of Telerik Document Processing Libraries. Access to the latest updates and support requires a valid license. Renew your license and download a new license key. Learn more about Telerik Document Processing Libraries licensing https://prgress.co/3PwQMut

Lauren Godfrey, Partner
322 North Shore Drive
Building 1B, Suite 200
Pittsburgh, Pennsylvania 15212
412-870-4129

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

October 21, 2026

VIA ONLINE SUBMISSION
Attorney General Nick Brown
Office of the Attorney General
Consumer Protection Division
1125 Washington Street SE
P.O. Box 40100
Olympia, WA 98504-0100

Re: Notification of Data Security Incident

To Whom It May Concern:

Constangy, Brooks, Smith & Prophete, LLP represents Dorsata, Inc., located at 240 W Main St., Suite 100-V62, Charlottesville, VA 22902-5009, in connection with its response to a recent data security incident discussed below. The purpose of this letter is to notify you of the incident in accordance with Washington data breach notification statute. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Dorsata, Inc. does not waive any rights or defenses regarding the applicability of Washington law, the applicability of the Washington data security incident notification statute, or personal jurisdiction.

1. Nature of the Security Incident

Dorsata, Inc. partners with women's health clinics and physicians to provide certain technology that is used in conjunction with healthcare provider's electronic health records system.

On August 12, 2026, we received a notice that the Metabase business intelligence software we use contained a security vulnerability. We immediately patched the software and began an investigation with the assistance of third-party cybersecurity experts. Our investigation determined the Metabase security vulnerability allowed unauthorized access to our database platform from August 10, 2026, to August 12, 2026. We reviewed the data involved in the incident and advised healthcare provider partners that protected health information was contained within the affected data. Dorsata, Inc. worked diligently to identify the individuals to whom that personal information related and to provide notification of the Incident to them on behalf of the healthcare partners.

Please note, we have no evidence of the misuse or attempted misuse of any accessible information.

Thank you for using version 2025.4.1104.462 of Telerik Document Processing Libraries. Access to the latest updates and support requires a valid license. Renew your license and download a new license key. Learn more about Telerik Document Processing Libraries licensing https://prgress.co/3PwQMut

2. Number of Affected Washington Residents & Information Involved

The incident involved personal information for approximately 1,993 Washington residents. The information involved in the incident for identified Washington residents included name, patient ID, medical history, treatment location, orders, provider name, and/or vaccines.

3. Notification to Identified Individuals

Between October 20, 2026 and October 21, 2026**,** notification letters were sent to identified Washington residents by USPS First Class Mail. The notification letter provides resources and steps individuals can take to help protect their information.

4. Measures Taken to Address the Incident

Upon identifying this incident, in addition to taking the steps described above, Dorsata, Inc. worked to learn more about what happened and what information could have been affected. Dorsata, Inc. notified the identified individuals and provided them with steps they can take to protect their personal information, including providing them with information about its toll-free call center established to answer questions about the incident and address related concerns.

5. Contact Information

If you have any questions or need additional information regarding this event, please do not hesitate to contact me at lgodfrey@constangy.com.

Sincerely,

Lauren D. Godfrey

Lauren D. Godfrey
Partner, Constangy, Brooks, Smith & Prophete LLP

Thank you for using version 2025.4.1104.462 of Telerik Document Processing Libraries. Access to the latest updates and support requires a valid license. Renew your license and download a new license key. Learn more about Telerik Document Processing Libraries licensing https://prgress.co/3PwQMut

Dorsata

[Return Address]
[Return City, State Zip]

To Enroll, Please Call: [TFN]
Or Visit: [URL]
Enrollment Code: [XXXXXX]

<<First Name>> <<Last Name>>
<<Address1>>
<<Address 2>>
<<City>>, <<State>> <<Zip Code>>

<<Date: Format (Month Day, Year)>>

Subject: Notice of Data [Variable Text 1: Security Incident / Breach]

Dear <<First Name>> <<Last Name>>:

We are writing to inform you of a recent data security incident involving a third-party software vendor, Metabase, that may have affected your protected health information. Dorsata, Inc. partners with women's health clinics and physicians to provide certain technology that is used in conjunction with your healthcare provider's electronic health records system. 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 August 12, 2026, we received a notice that the Metabase business intelligence software we use contained a security vulnerability. We immediately patched the software and began an investigation with the assistance of third-party cybersecurity experts. Our investigation determined the Metabase security vulnerability allowed unauthorized access to our database platform from August 10, 2026, to August 12, 2026. We reviewed the data involved in the incident and advised your healthcare provider that your protected health information was contained within the affected data. Your healthcare provider then requested that we notify you of the incident, which is the reason for this notification. Please note that we have no evidence of the misuse, or attempted misuse, of any potentially impacted information.

What Information Was Involved. The information may have included your name, [Variable Text 2: Affected Regulated Data Sets]. Your social security number was not involved.

What We Are Doing. As soon as we discovered this 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.

What You Can Do. You can follow the recommendations on the following page to help protect your information.

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 [Toll Free Number] Monday through Friday from [Insert Times]. We take your trust in us and this matter very seriously.

Please accept our sincere apologies for any worry or inconvenience this may cause.

Sincerely,
Dorsata, Inc.
240 W Main St.
Suite 100-V62
Charlottesville, VA 22902-5009

Thank you for using version 2025.4.1104.462 of Telerik Document Processing Libraries. Access to the latest updates and support requires a valid license. Renew your license and download a new license key. Learn more about Telerik Document Processing Libraries licensing https://prgress.co/3PwQMut

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
1510 Chester Pike
Crum Lynne, PA 19022
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

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
https://oag.maryland.gov
888-743-0023

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

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

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

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

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

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

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

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

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

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.

Thank you for using version 2025.4.1104.462 of Telerik Document Processing Libraries. Access to the latest updates and support requires a valid license. Renew your license and download a new license key. Learn more about Telerik Document Processing Libraries licensing https://prgress.co/3PwQMut

Lauren Godfrey, Partner
322 North Shore Drive
Building 1B, Suite 200
Pittsburgh, Pennsylvania 15212
412-870-4129

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

October 21, 2026

VIA ONLINE SUBMISSION
Attorney General Nick Brown
Office of the Attorney General
Consumer Protection Division
1125 Washington Street SE
P.O. Box 40100
Olympia, WA 98504-0100

Re: Notification of Data Security Incident

To Whom It May Concern:

Constangy, Brooks, Smith & Prophete, LLP represents Dorsata, Inc., located at 240 W Main St., Suite 100-V62, Charlottesville, VA 22902-5009, in connection with its response to a recent data security incident discussed below. The purpose of this letter is to notify you of the incident in accordance with Washington data breach notification statute. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Dorsata, Inc. does not waive any rights or defenses regarding the applicability of Washington law, the applicability of the Washington data security incident notification statute, or personal jurisdiction.

1. Nature of the Security Incident

Dorsata, Inc. partners with women's health clinics and physicians to provide certain technology that is used in conjunction with healthcare provider's electronic health records system.

On August 12, 2026, we received a notice that the Metabase business intelligence software we use contained a security vulnerability. We immediately patched the software and began an investigation with the assistance of third-party cybersecurity experts. Our investigation determined the Metabase security vulnerability allowed unauthorized access to our database platform from August 10, 2026, to August 12, 2026. We reviewed the data involved in the incident and advised healthcare provider partners that protected health information was contained within the affected data. Dorsata, Inc. worked diligently to identify the individuals to whom that personal information related and to provide notification of the Incident to them on behalf of the healthcare partners.

Please note, we have no evidence of the misuse or attempted misuse of any accessible information.

Thank you for using version 2025.4.1104.462 of Telerik Document Processing Libraries. Access to the latest updates and support requires a valid license. Renew your license and download a new license key. Learn more about Telerik Document Processing Libraries licensing https://prgress.co/3PwQMut

2. Number of Affected Washington Residents & Information Involved

The incident involved personal information for approximately 1,993 Washington residents. The information involved in the incident for identified Washington residents included name, patient ID, medical history, treatment location, orders, provider name, and/or vaccines.

3. Notification to Identified Individuals

Between October 20, 2026 and October 21, 2026**,** notification letters were sent to identified Washington residents by USPS First Class Mail. The notification letter provides resources and steps individuals can take to help protect their information.

4. Measures Taken to Address the Incident

Upon identifying this incident, in addition to taking the steps described above, Dorsata, Inc. worked to learn more about what happened and what information could have been affected. Dorsata, Inc. notified the identified individuals and provided them with steps they can take to protect their personal information, including providing them with information about its toll-free call center established to answer questions about the incident and address related concerns.

5. Contact Information

If you have any questions or need additional information regarding this event, please do not hesitate to contact me at lgodfrey@constangy.com.

Sincerely,

Lauren D. Godfrey

Lauren D. Godfrey
Partner, Constangy, Brooks, Smith & Prophete LLP

Thank you for using version 2025.4.1104.462 of Telerik Document Processing Libraries. Access to the latest updates and support requires a valid license. Renew your license and download a new license key. Learn more about Telerik Document Processing Libraries licensing https://prgress.co/3PwQMut

Dorsata

[Return Address]
[Return City, State Zip]

To Enroll, Please Call: [TFN]
Or Visit: [URL]
Enrollment Code: [XXXXXX]

<<First Name>> <<Last Name>>
<<Address1>>
<<Address 2>>
<<City>>, <<State>> <<Zip Code>>

<<Date: Format (Month Day, Year)>>

Subject: Notice of Data [Variable Text 1: Security Incident / Breach]

Dear <<First Name>> <<Last Name>>:

We are writing to inform you of a recent data security incident involving a third-party software vendor, Metabase, that may have affected your protected health information. Dorsata, Inc. partners with women's health clinics and physicians to provide certain technology that is used in conjunction with your healthcare provider's electronic health records system. 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 August 12, 2026, we received a notice that the Metabase business intelligence software we use contained a security vulnerability. We immediately patched the software and began an investigation with the assistance of third-party cybersecurity experts. Our investigation determined the Metabase security vulnerability allowed unauthorized access to our database platform from August 10, 2026, to August 12, 2026. We reviewed the data involved in the incident and advised your healthcare provider that your protected health information was contained within the affected data. Your healthcare provider then requested that we notify you of the incident, which is the reason for this notification. Please note that we have no evidence of the misuse, or attempted misuse, of any potentially impacted information.

What Information Was Involved. The information may have included your name, [Variable Text 2: Affected Regulated Data Sets]. Your social security number was not involved.

What We Are Doing. As soon as we discovered this 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.

What You Can Do. You can follow the recommendations on the following page to help protect your information.

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 [Toll Free Number] Monday through Friday from [Insert Times]. We take your trust in us and this matter very seriously.

Please accept our sincere apologies for any worry or inconvenience this may cause.

Sincerely,
Dorsata, Inc.
240 W Main St.
Suite 100-V62
Charlottesville, VA 22902-5009

Thank you for using version 2025.4.1104.462 of Telerik Document Processing Libraries. Access to the latest updates and support requires a valid license. Renew your license and download a new license key. Learn more about Telerik Document Processing Libraries licensing https://prgress.co/3PwQMut

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
1510 Chester Pike
Crum Lynne, PA 19022
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

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
https://oag.maryland.gov
888-743-0023

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

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

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

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

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

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

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

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

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

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.