

December 19, 2023

Via E-Mail: Idtheft@oag.state.md.us

Attorney General Brian E. Frosh
Office of the Attorney General
Identity Theft Unit
200 St. Paul Place
Baltimore, MD 21202

Re: ESO Solutions, Inc. - Data Security Incident

Dear Attorney General Frosh:

The undersigned represents ESO Solutions, Inc. (“ESO”), a provider of software services which help hospitals and healthcare systems improve operations, quality and patient outcomes. ESO was recently the victim of a sophisticated ransomware incident in which an unauthorized third party accessed and encrypted some of ESO’s computer systems. On behalf of ESO and the ESO customers listed below, we write to provide you notice of the incident and inform you that Maryland residents were impacted. This letter also explains the steps that have been taken to address the incident.

What Happened? On September 28, 2023, ESO detected and stopped a sophisticated ransomware incident, in which an unauthorized third party accessed and encrypted some of ESO’s computer systems. ESO immediately took the affected systems offline, secured its network environment, and engaged third-party forensic specialists to assist with investigating the extent of any unauthorized activity. ESO was ultimately able to confirm the security of its systems, safely restore its systems and operations via viable backups.

What Information was Impacted? On October 23, 2023, ESO determined that personal and patient health information was located on one of its impacted systems. This incident impacted data belonging to patients associated with ESO’s customers, including certain personal information and medical treatment information. This information included names, dates of birth, injury type, injury date, treatment date, treatment type and, in some cases, social security numbers.

With respect to customers that have authorized ESO to make regulatory disclosures on their behalf, the incident impacted the personal, medical or healthcare information of approximately 54,307 residents of this jurisdiction. The incident did not impact the Social Security Numbers of

33,813 of those residents notified in this jurisdiction.

Appendix A lists the impacted ESO customers that have requested that we provide notice to this office.

Steps ESO has taken. Immediately upon discovery of the incident, ESO secured its networks by taking the affected systems offline, implemented measures to confirm the security of its systems, engaged with a third-party forensic firm to assist in investigating the extent of the unauthorized activity and safely restored its systems and operations via viable backups. ESO also promptly notified the Federal Bureau of Investigation ("FBI") and has worked cooperatively with the FBI's investigation into this cyber-attack.

ESO has been in frequent communications with its impacted customers to support their response efforts. ESO first confirmed that medical and healthcare information was impacted beginning on or around October 23, 2023, and on an ongoing basis thereafter as its investigation progressed. ESO notified potentially impacted clients on a rolling basis beginning on December 12, 2023. See Exhibit A, Templates of Notification Letters.

ESO offered to support its impacted healthcare customers by offering to make any notifications the customers determined were required or appropriate. At the request and under the authorization of certain impacted clients, ESO notified prominent media outlets pursuant to 45 CFR § 164.406 on or around December 12, 2023. In addition, ESO notified the following entities beginning on or around December 18, 2023: the U.S. Department of Health and Human Services' Office for Civil Rights (OCR); certain state Attorneys General; and the consumer reporting agencies.

At the request and under the authorization of certain impacted clients, ESO will begin notifying impacted individuals on or around December 12, 2023. Impacted individuals will receive written notice pursuant to the enclosed notification letter template. Certain individuals will also receive substitute notice through the ESO's website at <https://www.eso.com/notice-of-cybersecurity-incident/>.

For more information: Please do not hesitate to contact us if you have any questions regarding this letter. You may also contact our impacted customers directly at the contacts listed in Appendix A.

Respectfully Submitted,
/s/ Maryam Meseha
MARYAM M. MESEHA, ESQ.
on behalf of FisherBroyles, LLP

Appendix A: Impacted ESO Customers Giving Notice to Maryland

Legal Entity and/or Healthcare System Name	Facility Name	Total Impacted Maryland Residents	Residents with Impacted SSNs
Baptist Memorial Health Care System	Baptist Memorial Hospital-Yazoo	1	0
	Baptist Memorial Hospital - DeSoto	5	1
	Baptist Memorial Hospital - North Mississippi	5	1
	Baptist Memorial Hospital - Golden Triangle	4	3
Bartlett Regional Hospital	Bartlett Regional Hospital	6	0
Boulder City Hospital	Boulder City Hospital	1	1
Baylor Scott & White Emergency Hospital - Aubrey (FKA Emerus Hospital East Denton County)	Dignity Health-St Rose Dominican San Martin Campus	1	1
	Dignity Health - St Rose Dominican Rose de Lima Campus	1	0
Community Health Systems	Merit Health Biloxi	1	1
	Jackson HMA LLC d/b/a Merit Health Central	2	1
	Merit Health River Oaks	1	0
ESO EMS Agency	UNC Hospitals Hillsborough Campus	2	0
	Mesa View Regional Hospital	2	1
	GW MFA George Washington Medical Facility	74	0
	ESO EMS Agency	54,109	20,430
Forrest Health	Forrest General Hospital	8	4
	Jefferson Davis Community Hospital	1	0
HCA Healthcare	Alaska Regional Hospital	12	0
Memorial Hospital at Gulfport Health System	Memorial Hospital at Gulfport	5	4
Miners Colfax Medical Center	Miners Colfax Medical Center	2	1
Providence St Joseph Health (AKA Providence)	Providence Alaska Medical Center	2	0
	Providence Seward Medical and Care Center	1	0
	Providence Valdez Medical Center	1	0
Regional One Health	Regional One Health	3	3
South Central Regional Medical Center	South Central Regional Medical Center	6	5
South Peninsula Hospital	South Peninsula Hospital	3	0
Universal Health Services (UHS)	Manatee Memorial Hospital	4	4
	Desert Springs Hospital Medical Center	1	0
University of Florida Health (FKA Shands Healthcare)	University of Florida Health in Jacksonville	21	17
	University of Florida Health (FKA Shands Healthcare)	22	16

Legal Entity and/or Healthcare System Name	Contact Information
Baptist Memorial Health Care System	Laura Cummins Email: laura.cummins@bmhcc.org Work phone: 901-227-4058
Bartlett Regional Hospital	Nathan Overson E-mail: noverson@bartletthospital.org Work phone: (907) 796-8578
Boulder City Hospital	Leigh Bohn E-mail: lbohnb@bchnv.org Work phone: (702) 293-4111
Baylor Scott & White Emergency Hospital - Aubrey (FKA Emerus Hospital East Denton County)	Laura Tautz Email: Linda.Tautz@emerus.com Work phone: 303-549-5099
Community Health Systems	Mary Kate Rigsbee Email: mary_rigsbee@chs.net Work phone: 601-339-9963
ESO EMS Agency	c/o FisherBroyles, LLP Maryam M. Mescha, Esq. Email: maryam.mescha@fisherbroyles.com Work phone: 609-250-2405
Forrest Health	Sandra Smith E-mail: sjsmith@forrestgeneral.com Work phone: (601) 288-4481
HCA Healthcare	<i>Alaska Regional Hospital</i> Charlyn Espejo-Monyer Email: Charlyn.Espejo@HCAhealthcare.com Phone: 907-264-1256
Memorial Hospital at Gulfport Health System	Wayne Cullinan E-mail: gcullinan@mhg.com Work phone: (228) 865-3178
Miners Colfax Medical Center	Terri Green E-mail: terri.green@mcme.nm.gov Work phone: (575) 445-7861
Providence St Joseph Health (AKA Providence)	Mary Jimenez Email: mary.jimenez@providence.org Work phone: Unknown
Regional One Health	Cheryl Rasbach E-mail: crasbach@regionalonehealth.org Work phone: (901) 545-6373
South Central Regional Medical Center	Ralph Heath Email: rheath@scrmc.com Work phone: Unknown
South Peninsula Hospital	Jim Bartilson E-mail: JMB@sphosp.org Work phone: (907) 235-0355
Universal Health Services (UHS)	Kyra Knapp Email: kyra.knapp@uhsinc.com Work phone: 970-397-5878
University of Florida Health (FKA Shands Healthcare)	Destiny Evans Email: deva0003@shands.ufl.edu Work phone: 352-627-9050

EXHIBIT A



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

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Notice of Data Incident

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

ESO Solutions, Inc. (“ESO”) provides software services that help hospitals and healthcare systems improve operations, quality, and patient outcomes. For this reason, we are likely to have your information from when a healthcare organization provided injury or emergency care to you in the past. We are writing to inform you of an incident that may have exposed your protected health information. We take the security of your information seriously and want to provide you with information you can use to help protect yourself.

What Happened

On September 28, 2023, we detected and stopped a sophisticated ransomware incident, in which an unauthorized third party accessed and encrypted some of ESO’s computer systems. We immediately took the affected systems offline, secured our network environment, and engaged third-party forensic specialists to assist us with investigating the extent of any unauthorized activity.

Our investigation determined that the unauthorized third party may have acquired your personal data during this incident. Please know that we have taken all reasonable steps to prevent your data from being further published or distributed, have notified and are working with federal law enforcement to investigate.

On October 23, 2023, we determined that your personal and patient information was located on one of the impacted systems. While we have found no evidence that your information has been misused, we are notifying you of this incident and offering you the resources provided in this letter, in an abundance of caution and so that you can take precautionary steps to help protect yourself, should you wish to do so. ESO recommends that you proceed with caution, and take advantage of the resources provided in this letter.

What Information Was Involved

At present there is no evidence that any of your personal information has been misused; however, the impacted data may have contained your personal information, including your name, social security number, phone number, address, and medical treatment information. Additionally, it is possible that the following protected health information fields could have been accessed: patient account and/or medical record number, injury and diagnosis information, procedure type (if applicable), insurance and payer information, and other items found in your registry file. At this time, we do not have evidence that your information has been misused.

What We Are Doing

Data security is one of our highest priorities. Upon discovery of the incident, we immediately secured our networks, implemented measures to confirm the security of our systems, safely restored our systems and operations via viable backups, initiated an investigation of the incident with the assistance of forensic experts, and notified the FBI (Federal Bureau of Investigation).

We value the safety of your personal information and want to make sure you have the information you need so that you can take steps to further protect yourself, should you feel it appropriate to do so. We encourage you to remain vigilant and to regularly review and monitor relevant account statements and credit reports and report suspected incidents of identity

theft to local law enforcement, your state's Attorney General, or the Federal Trade Commission (the "FTC"). We have included more information on these steps below.

In addition, we are providing you with access to 12 months of identity monitoring through Kroll at no charge to you.

What You Can Do

To help relieve concerns following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for 12 months. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6 (activation date)>> to activate your identity monitoring services.

Membership Number: <<Membership Number s_n>>

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Additional Steps

In addition to activating the complimentary identity monitoring services being offered, we encourage you to review the enclosed *Additional Important Information* for additional guidance on how to help protect against identify theft and fraud.

For More Information

On behalf of ESO, please accept our sincere apology for this incident and any inconvenience it may cause you. We value the security of the protected health information and personal information that we maintain, and understand the frustration, concern, and inconvenience that this incident may have caused. I can assure you that we continue to build on our already substantial investments in cybersecurity to prevent an incident like this from reoccurring and protect you and your information, now and in the future.

Representatives are available to assist you with questions regarding this incident, between the hours of 9:00 a.m. to 6:30 p.m. Eastern Time, Monday through Friday, excluding major U.S. holidays. Please call the help line at (866) 347-8525 with any questions you may have.

Sincerely,

Jonathan Cummings
Chief Information Security Officer
ESO

Additional Important Information

For residents of Hawaii, Michigan, Missouri, North Carolina, Vermont, Virginia, and Wyoming: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon, and West Virginia: It is required by state laws to inform you that 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.

For residents of Vermont: 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).

For residents of New Mexico: Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/documents/bcfr_consumer-rights-summary_2018-09.pdf, or by requesting information in writing from the Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

For residents of Washington, D.C.: You can obtain information about steps to take to avoid identity theft from the Office of the Attorney General for the District of Columbia at: 441 4th Street, NW, Washington, DC 20001; 202-727-3400; www.oag.dc.gov.

For residents of Iowa: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon: State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Maryland, Rhode Island, Illinois, New York, and North Carolina: You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft

Maryland Office of the Attorney General Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202
1-888-743-0023 www.oag.state.md.us

Rhode Island Office of the Attorney General Consumer Protection, 150 South Main Street, Providence, RI 02903
1-401-274-4400 www.riag.ri.gov

North Carolina Office of the Attorney General Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001 1-877-566-7226 www.ncdoj.com

Federal Trade Commission Consumer Response Center, 600 Pennsylvania Ave, NW Washington, DC 20580
1-877-IDTHEFT (438-4338) www.ftc.gov/idtheft

New York Office of Attorney General Consumer Frauds & Protection, The Capitol, Albany, NY 12224 1-800-771-7755
<https://ag.ny.gov/consumer-frauds/identity-theft>

For residents of Massachusetts and Rhode Island: It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of all states:

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 at the bottom of this page.

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

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

P.O. Box 105788
Atlanta, GA 30348 equifax.com/personal/credit-report-services/
1-800-349-9960

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013 experian.com/freeze/center.html
1-888-397-3742

TransUnion Security Freeze

P.O. Box 160
Woodlyn, PA 19094
transunion.com/credit-freeze
1-888-909-8872

More information can also be obtained by contacting the Federal Trade Commission listed above.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.



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

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Notice of Data Incident

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

ESO Solutions, Inc. (“ESO”) provides software services that help hospitals and healthcare systems improve operations, quality, and patient outcomes. For this reason, we are likely to have your information from when a healthcare organization provided injury or emergency care to you in the past. We are writing to inform you of an incident that may have exposed your protected health information. We take the security of your information seriously and want to provide you with information you can use to help protect yourself.

What Happened

On September 28, 2023, we detected and stopped a sophisticated ransomware incident, in which an unauthorized third party accessed and encrypted some of ESO’s computer systems. We immediately took the affected systems offline, secured our network environment, and engaged third-party forensic specialists to assist us with investigating the extent of any unauthorized activity.

Our investigation determined that the unauthorized third party may have acquired your personal data during this incident. Please know that we have taken all reasonable steps to prevent your data from being further published or distributed, have notified and are working with federal law enforcement to investigate.

On October 23, 2023, we determined that your personal and patient information was located on one of the impacted systems. While we have found no evidence that your information has been misused, we are notifying you of this incident and offering you the resources provided in this letter, in an abundance of caution and so that you can take precautionary steps to help protect yourself, should you wish to do so. ESO recommends that you proceed with caution, and take advantage of the resources provided in this letter.

What Information Was Involved

At present there is no evidence that any of your personal information has been misused; however, the impacted data may have contained your personal information, including your name, social security number, phone number, address, and medical treatment information. Additionally, it is possible that the following protected health information fields could have been accessed: patient account and/or medical record number, injury and diagnosis information, procedure type (if applicable), insurance and payer information, and other items found in your registry file. At this time, we do not have evidence that your information has been misused.

What We Are Doing

Data security is one of our highest priorities. Upon discovery of the incident, we immediately secured our networks, implemented measures to confirm the security of our systems, safely restored our systems and operations via viable backups, initiated an investigation of the incident with the assistance of forensic experts, and notified the FBI (Federal Bureau of Investigation).

We value the safety of your personal information and want to make sure you have the information you need so that you can take steps to further protect yourself, should you feel it appropriate to do so. We encourage you to remain vigilant and to regularly review and monitor relevant account statements and credit reports and report suspected incidents of identity

theft to local law enforcement, your state's Attorney General, or the Federal Trade Commission (the "FTC"). We have included more information on these steps below.

In addition, we are providing you with access to 24 months of identity monitoring through Kroll at no charge to you.

What You Can Do

To help relieve concerns following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for 24 months. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6 (activation date)>> to activate your identity monitoring services.

Membership Number: <<Membership Number s_n>>

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Additional Steps

In addition to activating the complimentary identity monitoring services being offered, we encourage you to review the enclosed *Additional Important Information* for additional guidance on how to help protect against identify theft and fraud.

For More Information

On behalf of ESO, please accept our sincere apology for this incident and any inconvenience it may cause you. We value the security of the protected health information and personal information that we maintain, and understand the frustration, concern, and inconvenience that this incident may have caused. I can assure you that we continue to build on our already substantial investments in cybersecurity to prevent an incident like this from reoccurring and protect you and your information, now and in the future.

Representatives are available to assist you with questions regarding this incident, between the hours of 9:00 a.m. to 6:30 p.m. Eastern Time, Monday through Friday, excluding major U.S. holidays. Please call the help line at (866) 347-8525 with any questions you may have.

Sincerely,

Jonathan Cummings
Chief Information Security Officer
ESO

Additional Important Information

For residents of Hawaii, Michigan, Missouri, North Carolina, Vermont, Virginia, and Wyoming: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon, and West Virginia: It is required by state laws to inform you that 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.

For residents of Vermont: 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).

For residents of New Mexico: Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/documents/bcfr_consumer-rights-summary_2018-09.pdf, or by requesting information in writing from the Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

For residents of Washington, D.C.: You can obtain information about steps to take to avoid identity theft from the Office of the Attorney General for the District of Columbia at: 441 4th Street, NW, Washington, DC 20001; 202-727-3400; www.oag.dc.gov.

For residents of Iowa: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon: State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Maryland, Rhode Island, Illinois, New York, and North Carolina: You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft

Maryland Office of the Attorney General Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202
1-888-743-0023 www.oag.state.md.us

Rhode Island Office of the Attorney General Consumer Protection, 150 South Main Street, Providence, RI 02903
1-401-274-4400 www.riag.ri.gov

North Carolina Office of the Attorney General Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001 1-877-566-7226 www.ncdoj.com

Federal Trade Commission Consumer Response Center, 600 Pennsylvania Ave, NW Washington, DC 20580
1-877-IDTHEFT (438-4338) www.ftc.gov/idtheft

New York Office of Attorney General Consumer Frauds & Protection, The Capitol, Albany, NY 12224 1-800-771-7755
<https://ag.ny.gov/consumer-frauds/identity-theft>

For residents of Massachusetts and Rhode Island: It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of all states:

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 at the bottom of this page.

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

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

P.O. Box 105788
Atlanta, GA 30348 equifax.com/personal/credit-report-services/
1-800-349-9960

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013 experian.com/freeze/center.html
1-888-397-3742

TransUnion Security Freeze

P.O. Box 160
Woodlyn, PA 19094
transunion.com/credit-freeze
1-888-909-8872

More information can also be obtained by contacting the Federal Trade Commission listed above.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.



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

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Notice of Data Incident

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

ESO Solutions, Inc. ("ESO") provides software services that help hospitals and healthcare systems improve operations, quality, and patient outcomes. For this reason, we are likely to have your information from when a healthcare organization provided injury or emergency care to you in the past. We are writing to inform you of an incident that may have exposed your protected health information. We take the security of your information seriously and want to provide you with information you can use to help protect yourself.

What Happened

On September 28, 2023, we detected and stopped a sophisticated ransomware incident, in which an unauthorized third party accessed and encrypted some of ESO's computer systems. We immediately took the affected systems offline, secured our network environment, and engaged third-party forensic specialists to assist us with investigating the extent of any unauthorized activity.

Our investigation determined that the unauthorized third party may have acquired your personal data during this incident. Please know that we have taken all reasonable steps to prevent your data from being further published or distributed, have notified and are working with federal law enforcement to investigate.

On October 23, 2023, we determined that your personal and patient information was located on one of the impacted systems. While we have found no evidence that your information has been misused, we are notifying you of this incident and offering you the resources provided in this letter, in an abundance of caution and so that you can take precautionary steps to help protect yourself, should you wish to do so. ESO recommends that you proceed with caution, and take advantage of the resources provided in this letter.

What Information Was Involved

Your social security number, claims information, and financial information **were not** impacted. It is possible that the following personal health information could have been accessed by an unauthorized third party: patient account and/or medical record number, injury and diagnosis information, procedure type (if applicable), insurance and payer information, and other items found in your registry file. At this time, we do not have evidence that your information has been misused.

What We Are Doing

Data security is one of our highest priorities. Upon discovery of the incident, we immediately secured our networks, implemented measures to confirm the security of our systems, safely restored our systems and operations via viable backups, initiated an investigation of the incident with the assistance of forensic experts, and notified the FBI (Federal Bureau of Investigation).

What You Can Do

We value the safety of your information and want to make sure you have the information you need so that you can take steps to further protect yourself, should you feel it appropriate to do so. We encourage you to remain vigilant and to regularly review and monitor relevant account statements and credit reports and report suspected incidents of identity theft to local law enforcement, your state's Attorney General, or the Federal Trade Commission (the "FTC"). We have included more information on these steps below.

While we do not believe any of your financial information was disclosed as a part of this event, we encourage you to review the enclosed *Additional Important Information* for information on how to protect against identify theft and fraud.

For More Information

On behalf of ESO, please accept our sincere apology for this incident and any inconvenience it may cause you. We value the security of the protected health information that we maintain, and understand the frustration, concern, and inconvenience that this incident may have caused. I can assure you that we continue to build on our already substantial investments in cybersecurity to prevent an incident like this from reoccurring and protect you and your information, now and in the future.

Representatives are available to assist you with questions regarding this incident, between the hours of 9:00 a.m. to 6:30 p.m. Eastern Time, Monday through Friday, excluding major U.S. holidays. Please call the help line at (866) 347-8525 with any questions you may have.

Sincerely,

Jonathan Cummings
Chief Information Security Officer
ESO

Additional Important Information

For residents of Hawaii, Michigan, Missouri, North Carolina, Vermont, Virginia, and Wyoming: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon, and West Virginia: It is required by state laws to inform you that 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.

For residents of Vermont: 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).

For residents of New Mexico: Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/documents/bcfr_consumer-rights-summary_2018-09.pdf, or by requesting information in writing from the Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

For residents of Washington, D.C.: You can obtain information about steps to take to avoid identity theft from the Office of the Attorney General for the District of Columbia at: 441 4th Street, NW, Washington, DC 20001; 202-727-3400; www.oag.dc.gov.

For residents of Iowa: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon: State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Maryland, Rhode Island, Illinois, New York, and North Carolina: You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft

Maryland Office of the Attorney General Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202
1-888-743-0023 www.oag.state.md.us

Rhode Island Office of the Attorney General Consumer Protection, 150 South Main Street, Providence, RI 02903
1-401-274-4400 www.riag.ri.gov

North Carolina Office of the Attorney General Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001 1-877-566-7226 www.ncdoj.com

Federal Trade Commission Consumer Response Center, 600 Pennsylvania Ave, NW Washington, DC 20580
1-877-IDTHEFT (438-4338) www.ftc.gov/idtheft

New York Office of Attorney General Consumer Frauds & Protection, The Capitol, Albany, NY 12224 1-800-771-7755
<https://ag.ny.gov/consumer-frauds/identity-theft>

For residents of Massachusetts and Rhode Island: It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of all states:

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 at the bottom of this page.

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

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

P.O. Box 105788
Atlanta, GA 30348 equifax.com/personal/credit-report-services/
1-800-349-9960

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013 experian.com/freeze/center.html
1-888-397-3742

TransUnion Security Freeze

P.O. Box 160
Woodlyn, PA 19094
transunion.com/credit-freeze
1-888-909-8872

More information can also be obtained by contacting the Federal Trade Commission listed above.



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

Parent or Guardian of

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>

<<address_1>>

<<address_2>>

<<city>>, <<state_province>> <<postal_code>>

<<country>>

Notice of Data Incident

Dear Parent or Guardian of <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

ESO Solutions, Inc. ("ESO") provides software services that help hospitals and healthcare systems improve operations, quality, and patient outcomes. For this reason, we are likely to have your child's information from when a healthcare organization provided injury or emergency care to your child in the past. We are writing to inform you of an incident that may have exposed your child's protected health information. We take the security of your child's information seriously and want to provide you with information you can use to help protect your child's information.

What Happened

On September 28, 2023, we detected and stopped a sophisticated ransomware incident, in which an unauthorized third party accessed and encrypted some of ESO's computer systems. We immediately took the affected systems offline, secured our network environment, and engaged third-party forensic specialists to assist us with investigating the extent of any unauthorized activity.

Our investigation determined that the unauthorized third party may have acquired your personal data during this incident. Please know that we have taken all reasonable steps to prevent your data from being further published or distributed, have notified and are working with federal law enforcement to investigate.

On October 23, 2023, we determined that your personal and patient information was located on one of the impacted systems. While we have found no evidence that your information has been misused, we are notifying you of this incident and offering you the resources provided in this letter, in an abundance of caution and so that you can take precautionary steps to help protect yourself, should you wish to do so. ESO recommends that you proceed with caution, and take advantage of the resources provided in this letter.

What Information Was Involved

At present there is no evidence that any of your child's personal information has been misused; however, the impacted data may have contained your child's personal information, including their name, social security number, phone number, address, and medical treatment information. Additionally, it is possible that the following protected health information fields could have been accessed: patient account and/or medical record number, injury and diagnosis information, procedure type (if applicable), insurance and payer information, and other items found in your child's registry file. At this time, we do not have evidence that your child's information has been misused.

What We Are Doing

Data security is one of our highest priorities. Upon discovery of the incident, we immediately secured our networks, implemented measures to confirm the security of our systems, safely restored our systems and operations via viable backups, initiated an investigation of the incident with the assistance of forensic experts, and notified the FBI (Federal Bureau of Investigation).

We value the safety of your child's personal information and want to make sure you have the information you need so that you can take steps to further protect your child's information, should you feel it appropriate to do so. We encourage you to remain vigilant and to regularly review and report suspected incidents of identity theft to local law enforcement,

your state's Attorney General, or the Federal Trade Commission (the "FTC"). We have included more information on these steps below.

In addition, we are providing you with access to 12 months of Minor Identity Monitoring through Kroll at no charge to you.

What You Can Do

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide Minor Identity Monitoring, Fraud Consultation, and Identity Theft Restoration at no cost to you or your child for 12 months. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your Minor Identity Monitoring services.

You have until <<b2b_text_6 (activation date)>> to activate your Minor Identity Monitoring services.

Membership Number: <<Membership Number s_n>>

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Additional Steps

In addition to activating the complimentary services being offered, please review the enclosed *Additional Important Information* section included with this letter. This section describes additional steps you can take to help protect your child's identity, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your child's credit file.

For More Information

On behalf of ESO, please accept our sincere apology for this incident and any inconvenience it may cause you. We value the security of the protected health information and personal information that we maintain, and understand the frustration, concern, and inconvenience that this incident may have caused. I can assure you that we continue to build on our already substantial investments in cybersecurity to prevent an incident like this from reoccurring and protect your child and your child's information, now and in the future.

Representatives are available to assist you with questions regarding this incident, between the hours of 9:00 a.m. to 6:30 p.m. Eastern Time, Monday through Friday, excluding major U.S. holidays. Please call the help line at (866) 347-8525 with any questions you may have.

Sincerely,

Jonathan Cummings
Chief Information Security Officer
ESO

Additional Important Information

For residents of Hawaii, Michigan, Missouri, North Carolina, Vermont, Virginia, and Wyoming: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon, and West Virginia: It is required by state laws to inform you that 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.

For residents of Vermont: 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).

For residents of New Mexico: Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/documents/bcfr_consumer-rights-summary_2018-09.pdf, or by requesting information in writing from the Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

For residents of Washington, D.C.: You can obtain information about steps to take to avoid identity theft from the Office of the Attorney General for the District of Columbia at: 441 4th Street, NW, Washington, DC 20001; 202-727-3400; www.oag.dc.gov.

For residents of Iowa: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon: State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Maryland, Rhode Island, Illinois, New York, and North Carolina: You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft

Maryland Office of the Attorney General Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202
1-888-743-0023 www.oag.state.md.us

Rhode Island Office of the Attorney General Consumer Protection, 150 South Main Street, Providence, RI 02903
1-401-274-4400 www.riag.ri.gov

North Carolina Office of the Attorney General Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001 1-877-566-7226 www.ncdoj.com

Federal Trade Commission Consumer Response Center, 600 Pennsylvania Ave, NW Washington, DC 20580
1-877-IDTHEFT (438-4338) www.ftc.gov/idtheft

New York Office of Attorney General Consumer Frauds & Protection, The Capitol, Albany, NY 12224 1-800-771-7755
<https://ag.ny.gov/consumer-frauds/identity-theft>

For residents of Massachusetts and Rhode Island: It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of all states:

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 at the bottom of this page.

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

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

P.O. Box 105788
Atlanta, GA 30348 [equifax.com/
personal/credit-report-services/](http://equifax.com/personal/credit-report-services/)
1-800-349-9960

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013 [experian.com/
freeze/center.html](http://experian.com/freeze/center.html)
1-888-397-3742

TransUnion Security Freeze

P.O. Box 160
Woodlyn, PA 19094
transunion.com/credit-freeze
1-888-909-8872

More information can also be obtained by contacting the Federal Trade Commission listed above.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Minor Identity Monitoring

Minor Identity Monitoring detects when names, addresses, and credit information is associated with your child's Social Security number. An alert will be sent to you when activity is detected. The presence of a credit file may be an indicator of identity theft or fraud for children who, as minors, should not have a credit history.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To activate services, a U.S. Social Security number and U.S. residential address is required.



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

Parent or Guardian of

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>

<<address_1>>

<<address_2>>

<<city>>, <<state_province>> <<postal_code>>

<<country>>

Notice of Data Incident

Dear Parent or Guardian of <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

ESO Solutions, Inc. ("ESO") provides software services that help hospitals and healthcare systems improve operations, quality, and patient outcomes. For this reason, we are likely to have your child's information from when a healthcare organization provided injury or emergency care to your child in the past. We are writing to inform you of an incident that may have exposed your child's protected health information. We take the security of your child's information seriously and want to provide you with information you can use to help protect your child's information.

What Happened

On September 28, 2023, we detected and stopped a sophisticated ransomware incident, in which an unauthorized third party accessed and encrypted some of ESO's computer systems. We immediately took the affected systems offline, secured our network environment, and engaged third-party forensic specialists to assist us with investigating the extent of any unauthorized activity.

Our investigation determined that the unauthorized third party may have acquired your personal data during this incident. Please know that we have taken all reasonable steps to prevent your data from being further published or distributed, have notified and are working with federal law enforcement to investigate.

On October 23, 2023, we determined that your personal and patient information was located on one of the impacted systems. While we have found no evidence that your information has been misused, we are notifying you of this incident and offering you the resources provided in this letter, in an abundance of caution and so that you can take precautionary steps to help protect yourself, should you wish to do so. ESO recommends that you proceed with caution, and take advantage of the resources provided in this letter.

What Information Was Involved

At present there is no evidence that any of your child's personal information has been misused; however, the impacted data may have contained your child's personal information, including their name, social security number, phone number, address, and medical treatment information. Additionally, it is possible that the following protected health information fields could have been accessed: patient account and/or medical record number, injury and diagnosis information, procedure type (if applicable), insurance and payer information, and other items found in your child's registry file. At this time, we do not have evidence that your child's information has been misused.

What We Are Doing

Data security is one of our highest priorities. Upon discovery of the incident, we immediately secured our networks, implemented measures to confirm the security of our systems, safely restored our systems and operations via viable backups, initiated an investigation of the incident with the assistance of forensic experts, and notified the FBI (Federal Bureau of Investigation).

We value the safety of your child's personal information and want to make sure you have the information you need so that you can take steps to further protect your child's information, should you feel it appropriate to do so. We encourage you to remain vigilant and to regularly review and report suspected incidents of identity theft to local law enforcement,

your state's Attorney General, or the Federal Trade Commission (the "FTC"). We have included more information on these steps below.

In addition, we are providing you with access to 24 months of Minor Identity Monitoring through Kroll at no charge to you.

What You Can Do

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide Minor Identity Monitoring, Fraud Consultation, and Identity Theft Restoration at no cost to you or your child for 24 months. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your Minor Identity Monitoring services.

You have until <<b2b_text_6 (activation date)>> to activate your Minor Identity Monitoring services.

Membership Number: <<Membership Number s_n>>

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Additional Steps

In addition to activating the complimentary services being offered, please review the enclosed *Additional Important Information* section included with this letter. This section describes additional steps you can take to help protect your child's identity, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your child's credit file.

For More Information

On behalf of ESO, please accept our sincere apology for this incident and any inconvenience it may cause you. We value the security of the protected health information and personal information that we maintain, and understand the frustration, concern, and inconvenience that this incident may have caused. I can assure you that we continue to build on our already substantial investments in cybersecurity to prevent an incident like this from reoccurring and protect your child and your child's information, now and in the future.

Representatives are available to assist you with questions regarding this incident, between the hours of 9:00 a.m. to 6:30 p.m. Eastern Time, Monday through Friday, excluding major U.S. holidays. Please call the help line at (866) 347-8525 with any questions you may have.

Sincerely,

Jonathan Cummings
Chief Information Security Officer
ESO

Additional Important Information

For residents of Hawaii, Michigan, Missouri, North Carolina, Vermont, Virginia, and Wyoming: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon, and West Virginia: It is required by state laws to inform you that 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.

For residents of Vermont: 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).

For residents of New Mexico: Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/documents/bcfr_consumer-rights-summary_2018-09.pdf, or by requesting information in writing from the Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

For residents of Washington, D.C.: You can obtain information about steps to take to avoid identity theft from the Office of the Attorney General for the District of Columbia at: 441 4th Street, NW, Washington, DC 20001; 202-727-3400; www.oag.dc.gov.

For residents of Iowa: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon: State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Maryland, Rhode Island, Illinois, New York, and North Carolina: You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft

Maryland Office of the Attorney General Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202
1-888-743-0023 www.oag.state.md.us

Rhode Island Office of the Attorney General Consumer Protection, 150 South Main Street, Providence, RI 02903
1-401-274-4400 www.riag.ri.gov

North Carolina Office of the Attorney General Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001 1-877-566-7226 www.ncdoj.com

Federal Trade Commission Consumer Response Center, 600 Pennsylvania Ave, NW Washington, DC 20580
1-877-IDTHEFT (438-4338) www.ftc.gov/idtheft

New York Office of Attorney General Consumer Frauds & Protection, The Capitol, Albany, NY 12224 1-800-771-7755
<https://ag.ny.gov/consumer-frauds/identity-theft>

For residents of Massachusetts and Rhode Island: It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of all states:

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 at the bottom of this page.

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

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

P.O. Box 105788
Atlanta, GA 30348 [equifax.com/
personal/credit-report-services/](http://equifax.com/personal/credit-report-services/)
1-800-349-9960

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013 [experian.com/
freeze/center.html](http://experian.com/freeze/center.html)
1-888-397-3742

TransUnion Security Freeze

P.O. Box 160
Woodlyn, PA 19094
transunion.com/credit-freeze
1-888-909-8872

More information can also be obtained by contacting the Federal Trade Commission listed above.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Minor Identity Monitoring

Minor Identity Monitoring detects when names, addresses, and credit information is associated with your child's Social Security number. An alert will be sent to you when activity is detected. The presence of a credit file may be an indicator of identity theft or fraud for children who, as minors, should not have a credit history.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To activate services, a U.S. Social Security number and U.S. residential address is required.



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

Parent or Guardian of

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>

<<address_1>>

<<address_2>>

<<city>>, <<state_province>> <<postal_code>>

<<country>>

Notice of Data Incident

Dear Parent or Guardian of <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

ESO Solutions, Inc. ("ESO") provides software services that help hospitals and healthcare systems improve operations, quality, and patient outcomes. For this reason, we are likely to have your child's information from when a healthcare organization provided injury or emergency care to your child in the past. We are writing to inform you of an incident that may have exposed your child's protected health information. We take the security of your child's information seriously and want to provide you with information you can use to help protect your child's information.

What Happened

On September 28, 2023, we detected and stopped a sophisticated ransomware incident, in which an unauthorized third party accessed and encrypted some of ESO's computer systems. We immediately took the affected systems offline, secured our network environment, and engaged third-party forensic specialists to assist us with investigating the extent of any unauthorized activity.

Our investigation determined that the unauthorized third party may have acquired your personal data during this incident. Please know that we have taken all reasonable steps to prevent your data from being further published or distributed, have notified and are working with federal law enforcement to investigate.

On October 23, 2023, we determined that your personal and patient information was located on one of the impacted systems. While we have found no evidence that your information has been misused, we are notifying you of this incident and offering you the resources provided in this letter, in an abundance of caution and so that you can take precautionary steps to help protect yourself, should you wish to do so. ESO recommends that you proceed with caution, and take advantage of the resources provided in this letter.

What Information Was Involved

Your child's social security number, claims information, and financial information associated with payment **were not** impacted. It is possible that the following personal health information could have been accessed by an unauthorized third party: patient account and/or medical record number, injury and diagnosis information, procedure type (if applicable), insurance and payer information, and other items found in your registry file. At this time, we do not have evidence that your child's information has been misused or shared.

What We Are Doing

Data security is one of our highest priorities. Upon discovery of the incident, we immediately secured our networks, implemented measures to confirm the security of our systems, safely restored our systems and operations via viable backups, initiated an investigation of the incident with the assistance of forensic experts, and notified the FBI (Federal Bureau of Investigation).

What You Can Do

We value the safety of your child's information and want to make sure you have the information you need so that you can take steps to further protect your child's information, should you feel it appropriate to do so. We encourage you to remain vigilant and to regularly review and monitor your child's relevant accounts and report suspected incidents of identity theft to local law enforcement, your state's Attorney General, or the Federal Trade Commission (the "FTC"). We have included more information on these steps below.

While we do not believe any of your financial information related to your child's patient information was disclosed as a part of this event, we encourage you to review the enclosed *Additional Important Information* for information on how to protect against identify theft and fraud.

For More Information

On behalf of ESO, please accept our sincere apology for this incident and any inconvenience it may cause you. We value the security of the protected health information that we maintain, and understand the frustration, concern, and inconvenience that this incident may have caused. I can assure you that we continue to build on our already substantial investments in cybersecurity to prevent an incident like this from reoccurring and protect you and your information, now and in the future.

Representatives are available to assist you with questions regarding this incident, between the hours of 9:00 a.m. to 6:30 p.m. Eastern Time, Monday through Friday, excluding major U.S. holidays. Please call the help line at (866) 347-8525 with any questions you may have.

Sincerely,

Jonathan Cummings
Chief Information Security Officer
ESO

Additional Important Information

For residents of Hawaii, Michigan, Missouri, North Carolina, Vermont, Virginia, and Wyoming: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon, and West Virginia: It is required by state laws to inform you that 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.

For residents of Vermont: 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).

For residents of New Mexico: Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/documents/bcfr_consumer-rights-summary_2018-09.pdf, or by requesting information in writing from the Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

For residents of Washington, D.C.: You can obtain information about steps to take to avoid identity theft from the Office of the Attorney General for the District of Columbia at: 441 4th Street, NW, Washington, DC 20001; 202-727-3400; www.oag.dc.gov.

For residents of Iowa: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon: State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Maryland, Rhode Island, Illinois, New York, and North Carolina: You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft

Maryland Office of the Attorney General Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202
1-888-743-0023 www.oag.state.md.us

Rhode Island Office of the Attorney General Consumer Protection, 150 South Main Street, Providence, RI 02903
1-401-274-4400 www.riag.ri.gov

North Carolina Office of the Attorney General Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001 1-877-566-7226 www.ncdoj.com

Federal Trade Commission Consumer Response Center, 600 Pennsylvania Ave, NW Washington, DC 20580
1-877-IDTHEFT (438-4338) www.ftc.gov/idtheft

New York Office of Attorney General Consumer Frauds & Protection, The Capitol, Albany, NY 12224 1-800-771-7755
<https://ag.ny.gov/consumer-frauds/identity-theft>

For residents of Massachusetts and Rhode Island: It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of all states:

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 at the bottom of this page.

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

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

P.O. Box 105788
Atlanta, GA 30348 [equifax.com/
personal/credit-report-services/](http://equifax.com/personal/credit-report-services/)
1-800-349-9960

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013 [experian.com/
freeze/center.html](http://experian.com/freeze/center.html)
1-888-397-3742

TransUnion Security Freeze

P.O. Box 160
Woodlyn, PA 19094
transunion.com/credit-freeze
1-888-909-8872

More information can also be obtained by contacting the Federal Trade Commission listed above.



PIERSON FERDINAND

MARYAM M. MESEHA, ESQ.
FOUNDING PARTNER

Mail

11010 Lake Grove Boulevard, Suite 100-167
Morrisville, NC 27560

Office

525 North Tryon Street, Suite 1600
Charlotte, NC 29202

Direct: 973.419.7819

Email: Maryam.meseha@pierferd.com

April 8, 2024

Via E-Mail: Idtheft@oag.state.md.us

Attorney General Brian E. Frosh
Office of the Attorney General
Identity Theft Unit
200 St. Paul Place
Baltimore, MD 21202

Re: ESO Solutions, Inc. - Data Security Incident

Dear Attorney General Frosh:

As you are aware, the undersigned represents ESO Solutions, Inc. (“ESO”), a provider of software services which help hospitals and healthcare systems improve operations, quality, and patient outcomes. On December 18, 2023, ESO provided you notice of a security incident and informed you that Maryland residents were impacted.

This incident impacted data belonging to patients associated with ESO’s customers, including certain personal information and medical treatment information. Since that time, ESO has continued to issue notification on a rolling basis to impacted individuals up to and including on March 1, 2024.

Please accept this letter as a supplement to our prior notification intended to update you on the amount of residents notified in this jurisdiction. With respect to customers that have authorized ESO to make regulatory disclosures on their behalf, the incident impacted the personal, medical or healthcare information of approximately 70,884 residents of this jurisdiction. The incident did not impact the Social Security Numbers or financial account information of 34,925 of those residents notified in this jurisdiction.

Appendix A lists the impacted ESO customers that have requested that we provide notice to this office.

For more information: Please do not hesitate to contact us if you have any questions regarding this letter. You may also contact our impacted customers directly at the contacts listed in Appendix A.

Very truly yours,



PIERSON FERDINAND

/s/ Maryam Meseha

Maryam M. Meseha, Esq.

April 8, 2024

Page 2 of 5

Appendix A: Impacted ESO Customers Giving Notice to Maryland

Facility Name	Residents with Impacted SSNs	Total Impacted Maryland Residents
Alaska Regional Hospital	0	15
Anderson Regional Medical Center North	1	1
Ascension Sacred Heart Bay Medical	1	1
Ascension Seton Hays	0	1
Ascension Seton Williamson	2	2
Atrium Health Cabarrus	0	14
Atrium Health Carolinas Medical Center	0	49
Atrium Health Cleveland	0	2
Atrium Health Wake Forest Baptist	0	9
Aventura Hospital and Medical Center	1	9
Banner Churchill Hospital EMS	0	1
Baptist Health Care Inc successor by merger of Baptist Hospital Inc and Baptist Health Care Corporation	10	10
Baptist Memorial Hospital - DeSoto	1	5
Baptist Memorial Hospital - Golden Triangle	7	8
Baptist Memorial Hospital - North Mississippi	1	6
Baptist Memorial Hospital-Yazoo	0	1
Bartlett Regional Hospital	0	6
Bayfront Health Brooksville	1	1
Bayfront Health St Petersburg	35	35
Blake Medical Center	8	8
Boulder City Hospital	1	1
Brandon Regional Hospital	1	1
Capital Regional Medical Center	1	2
Central Florida Regional Hospital (HCA FL Lake Monroe)	0	1
Dell Children's Medical Center of Central Texas	0	1
Dell Seton Medical Center at The University of Texas (Brackenridge)	3	9
Delray Medical Center	21	21
Desert Springs Hospital Medical Center	0	1
Dignity Health - St Rose Dominican Rose de Lima Campus	0	1
Dignity Health-St Rose Dominican San Martin Campus	1	1
Doctors Hospital of Sarasota	1	1
Duke University Hospital (NC)	0	1
ECU Medical Center	0	106
Englewood Community Hospital	2	3

April 8, 2024

Page 3 of 5

ESO EMS Agency	35383	69884
Fawcett Memorial Hospital	3	4
Forrest General Hospital	5	11
Fort Walton Beach Medical Center	1	1
Gallup Indian Medical Center	0	1
Good Samaritan Medical Center	1	1
Gulf Breeze Hospital	1	1
Gulf Coast Regional Medical Center	1	1
Halifax Health	40	40
HCA FL Citrus Hospital	0	1
HCA Florida North Florida Hospital	4	6
HCA Florida Ocala	6	17
Health First Cape Canaveral Hospital	9	9
Health First Holmes Regional Medical Center	64	64
Hendry Regional Medical Center	1	1
Highland Community Hospital	1	1
Jackson HMA LLC d/b/a Merit Health Central	1	2
Jacksonville Memorial Hospital	0	2
Jefferson Davis Community Hospital	0	1
JFK MEDICAL CENTER	12	14
JFK Medical Center - North	1	1
Kendall Regional Medical Center	5	12
Lake City Medical Center	2	3
Lakeland Regional Health Medical Center	12	12
Largo Medical Center	7	10
Lawnwood Regional Medical Center and Heart Institute	20	28
Lee Memorial Hospital	14	14
Lower Keys Medical Center	9	9
Manatee Memorial Hospital	5	5
Mat-Su Regional Medical Center	0	1
Medical Center of Trinity	1	2
Melbourne Regional Medical Center	5	5
Memorial Hospital at Gulfport	7	8
Memorial Regional Hospital	7	7
Merit Health Biloxi	5	5
Merit Health River Oaks	1	2
MetroHealth Cleveland Heights Medical Center	0	2
MH Mission Hospital, LLLP	0	28

April 8, 2024

Page 4 of 5

Miners Colfax Medical Center	1	2
Mount Sinai Medical Center	8	9
Neshoba County General Hospital	2	2
Northside Hospital & Tampa Bay Heart Institute	0	1
Northside Hospital and Tampa Bay Heart Institute	1	1
Northwest Medical Center	2	2
Oak Hill Hospital	3	4
OCH Regional Medical Center	3	3
Orange Park Medical Center	7	8
Orlando Health	30	30
Orlando Health - St Cloud Regional Medical Center	1	1
Palm Bay Hospital	6	6
Palms of Pasadena Hospital	1	1
Palms West Hospital	2	2
Physicians Regional - Collier Boulevard	1	1
Physicians Regional - Pine Ridge	4	4
Plantation General Hospital	2	2
Poinciana Medical Center	0	1
Presbyterian Hospital	1	1
Providence Alaska Medical Center	0	4
Providence Seward Medical and Care Center	0	1
Providence Valdez Medical Center	0	1
Putnam Community Medical Center	0	2
Raulerson Hospital	2	2
Regional Medical Center - North	1	1
Regional Medical Center Bayonet Point	8	8
Regional One Health	3	3
Rockledge Regional Medical Center	10	10
SACRED HEART HOSPITAL	3	3
SARASOTA MEMORIAL HOSPITAL - TC	9	9
Sebastian River Medical Center	2	2
Shorepoint (Bayfront) Health Port Charlotte	3	3
Shorepoint (Bayfront) Health Punta Gorda	2	2
SIERRA VISTA HOSPITAL	0	1
South Bay Hospital	2	2
South Central Regional Medical Center	5	6
South Peninsula Hospital	0	5
St Lucie Medical Center	2	2



April 8, 2024

Page 5 of 5

ST MARYS MEDICAL CENTER	32	32
St Mary's Medical Center (FL)	3	3
St. Petersburg General Hospital	1	3
Tallahassee Memorial Healthcare	6	6
Tampa General Hospital	10	10
Twin Cities Hospital	2	2
UNIVERSITY HOSPITAL AND MEDICAL CENTER	0	3
University of Florida Health (FKA Shands Healthcare)	21	27
University of Florida Health in Jacksonville	17	21
University of Mississippi Medical Center	1	1
University of New Mexico Hospitals (Dup of UNM account)	0	15
WakeMed Cary Hospital	0	4
WakeMed Raleigh Campus (NC)	0	50
West Boca Medical Center	1	1
WEST FLORIDA HOSPITAL	0	1
West Marion Community Hospital	3	5
Westside Regional Medical Center	2	2