

16023



**AEGIS MEDICAL GROUP**

C/O ID Experts  
PO Box 4219  
Everett WA 98204

To Enroll, Please Call:  
1-833-953-1383  
Or Visit:  
<https://ide.myidcare.com/amg>  
Enrollment Code: <<ENROLLCODE>>

ENDORSE



NAME

ADDRESS1

ADDRESS2

CSZ

BREAK

November 8, 2019

SEQ  
CODE 2D COUNTRY  
Ver VERS

**Notice of Data Breach**

Dear <<First Name>> <<Last Name>>,

This notice is sent to you on behalf of Aegis Medical Group ("Aegis") to alert you to an important matter.

**What Happened**

On September 11, 2019 Aegis became aware from law enforcement that a former employee inappropriately accessed certain patient account information maintained by Aegis prior to Aegis's termination of that former employee. It appears that the former employee attempted to sell certain account information to third parties who may have been engaged in some form of attempted identity theft or financial fraud. We believe the improper access occurred between July 24, 2019 and September 9, 2019.

**What Information Was Involved**

You are receiving this notice because you are either a former or current patient of Aegis Medical Group. As of the date of this notice, law enforcement has identified to the company only two (2) Aegis patients whose personal information the former employee attempted to sell. While Aegis is uncertain whether any of your specific account information was actually accessed by the former employee, the records that were potentially subject to unauthorized access included the following information: patients' first and last name, Social Security number, date of birth, account number, mailing address and diagnosis.

**What We Are Doing**

We have reviewed our relevant policies and procedures, and we have taken steps to minimize the risk of future incidents. We estimate that approximately seventy-five percent (75%) of the potentially exposed records were non-electronic paper records. Although the paper records were properly stored, Aegis is undertaking a process to convert additional paper records to an electronic format. This effort will allow Aegis to better control and restrict access to account records. In addition, upon learning of this incident we also immediately terminated the employee who inappropriately accessed and misused account records.

Aegis has also made its employees aware of this incident and the consequences to the individual involved and has reminded its employees of the importance of maintaining the security and confidentiality of individual patient account records.

In addition, we are offering identity theft protection services through ID Experts®, the data breach and recovery services expert, to provide you with MyIDCare™. MyIDCare services include: 12 months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity is compromised.

## What You Can Do

We advise you to remain vigilant and monitor your credit reports periodically. The Fair Credit Reporting Act requires each of the nationwide consumer reporting companies (Equifax, Experian and TransUnion) to provide you with a free copy of your credit report, at your request, once every 12 months. To order, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call 1-877-322-8228. The enclosed Recommended Steps document provides additional information on other precautions you may want to consider.

If you have reason to believe that any of your personal information is being misused, you should contact local law enforcement (including your State Attorney General's Office) and file a police report. Creditors may want a copy of the police report to absolve you of any fraudulent debts.

As noted above, we have arranged a credit monitoring service for up to 12 months to be made available to you through ID Experts. We encourage you to contact ID Experts with any questions and to enroll in free MyIDCare services by calling 1-833-953-1383 or going to <https://ide.myidcare.com/amg> and using the Enrollment Code provided above. MyIDCare representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is February 8, 2020.

Although the chances that your individual information was misused are very small, we encourage you to take full advantage of this service offering. MyIDCare representatives have been informed about the incident and can answer questions you may have regarding this incident and the free MyIDCare services.

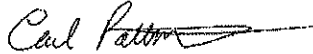
You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the Enrollment Code at the top of this letter when calling or enrolling online, so please do not discard this letter.

## For More Information

Please call 1-833-953-1383 toll-free or go to <https://ide.myidcare.com/amg> for assistance or for any additional questions you may have concerning this incident.

Please be assured that we take our responsibility to protect sensitive personal information seriously and we apologize for any inconvenience this incident may cause you.

Sincerely,



Carl Patten  
Aegis Medical Group

(Enclosure)



### Recommended Steps to Help Protect Your Information

- 1. Website and Enrollment.** Go to <https://ide.myidcare.com/amg> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.
- 2. Activate the credit monitoring** provided as part of your MyIDCare membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, MyIDCare will be able to assist you.
- 3. Telephone.** Contact MyIDCare at 1-833-953-1383 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.
- 4. Review your credit reports.** We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to [www.annualcreditreport.com](http://www.annualcreditreport.com) or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in MyIDCare, notify them immediately by calling or by logging into the MyIDCare website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

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

**5. Place Fraud Alerts** with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. 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. The contact information for all three bureaus is as follows:

#### Credit Bureaus

Equifax Fraud Reporting  
1-866-349-5191  
P.O. Box 105069  
Atlanta, GA 30348-5069  
[www.equifax.com](http://www.equifax.com)

Experian Fraud Reporting  
1-888-397-3742  
P.O. Box 9554  
Allen, TX 75013  
[www.experian.com](http://www.experian.com)

TransUnion Fraud Reporting  
1-800-680-7289  
P.O. Box 2000  
Chester, PA 19022-2000  
[www.transunion.com](http://www.transunion.com)

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

**Please Note: No one is allowed to place a fraud alert on your credit report except you.**

**6. Security Freeze.** By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

**7. You can obtain additional information** about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

**Kentucky Residents:** Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, [www.ag.ky.gov](http://www.ag.ky.gov), Telephone: 1-502-696-5300.

**Maryland Residents:** Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place Baltimore, MD 21202, [www.oag.state.md.us/Consumer](http://www.oag.state.md.us/Consumer), Telephone: 1-888-743-0023.

**North Carolina Residents:** Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, [www.ncdoj.gov](http://www.ncdoj.gov), Telephone: 1-919-716-6400.

**All US Residents:** Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft), 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.

Breach Tracking Number: 5773N4VRBF

Thank you for filing a breach notification via the website of the Office for Civil Rights (OCR) at the Department of Health and Human Services. This is an automated response to acknowledge receipt of your breach notification. Your breach notification will be assigned to an OCR staff member for review and appropriate action. If OCR has any questions about the breach notification you submitted, we will contact you directly. Otherwise, you will receive a written response indicating whether or not OCR has accepted your breach notification for investigation.

**Please do not fax, email, or mail a copy of this breach notification to us as that may delay the processing of your breach notification.**

If you have any additional information to add to your breach notification, you may call 1-800-368-1019. Please reference the number given by OCR when submitting your breach notification.

\* Breach Affecting: 500 or More Individuals

\* Report Type: Initial Breach Report

\* Are you a Covered Entity filing on behalf of your organization? Yes

**Covered Entity**

\* Name of Covered Entity: Aegis Medical Group

\* Type of Covered Entity: Healthcare Provider

\* Street Address Line 1: 711 N 3rd Street

Street Address Line 2: Suite 2

\* City: Leesburg

\* State: Florida

\* ZIP: 34748

**Covered Entity Point of Contact Information**

\* First Name: Carl \* Last Name: Patten

\* Email: cpatten@aegismedicalgroup.com

Contact Phones

\* Phone Number: **Phone Number Usage**

(Include area code): (352) 720-0940 Work

(888) 701-7172 Work

\* Breach Start Date: 07/24/2019 \* Breach End Date: 09/09/2019

\* Discovery Start Date: 09/11/2019 \* Discovery End Date: 10/25/2019

\* Approximate Number of Individuals Affected by the Breach: 9800

\* Type of Breach: Unauthorized Access/Disclosure

\* Location of Breach: Electronic Medical Record  
Laptop  
Network Server  
Paper/Films

**Clinical  
Demographic  
Financial**

\* Clinical

Diagnosis/Conditions  
Lab Results  
Medications  
Other Treatment Information

\* Type of Protected Health Information Involved in Breach:

\* Demographic

Address/ZIP  
Date of Birth  
Drivers License  
Name  
SSN

\* Financial

Claims Information

\* Brief Description of the Breach:

On September 11, 2019 Aegis became aware from law enforcement that a former employee inappropriately accessed certain patient account information maintained by Aegis prior to Aegis's termination of that former employee. It appears that the former employee attempted to sell certain account information to third parties who may have been engaged in some form of attempted identity theft or financial fraud. We believe the improper access occurred between July 24, 2019 and September 9, 2019.

\* Safeguards in Place Prior to Breach:

Privacy Rule Safeguards (Training, Policies and Procedures, etc.)  
Security Rule Administrative Safeguards (Risk Analysis, Risk Management, etc.)  
Security Rule Physical Safeguards (Facility Access Controls, Workstation Security, etc.)  
Security Rule Technical Safeguards (Access Controls, Transmission Security, etc.)

\* Individual Notice Provided Start Date:

11/08/2019

Individual Notice Provided  
Projected/Expected End Date: 11/08/2019

Was Substitute Notice Required?

Yes

10 or more

Was Media Notice Required?

Yes

\* Select State(s) and/or

Florida

11/7/2019

Territories in which media notice was provided:

---

\* Actions Taken in Response to Breach:

- Implemented new technical safeguards
- Provided individuals with free credit monitoring
- Revised policies and procedures
- Sanctioned workforce members involved (including termination)
- Took steps to mitigate harm
- Trained or retrained workforce members
- Other

\* Describe Other Actions Taken:

Proactively working with law enforcement to investigate the information the former employee attempted to actually sell. As of November 7, law enforcement has identified two (2) patients of this organization whose information the former employee attempted to sell.

Under the Freedom of Information Act (5 U.S.C. §552) and HHS regulations at 45 C.F.R. Part 5, OCR may be required to release information provided in your breach notification. For breaches affecting more than 500 individuals, some of the information provided on this form will be made publicly available by posting on the HHS web site pursuant to § 13402(e)(4) of the Health Information Technology for Economic and Clinical Health (HITECH) Act (Pub. L. 111-5). Additionally, OCR will use this information, pursuant to § 13402(i) of the HITECH Act, to provide an annual report to Congress regarding the number and nature of breaches that are reported each year and the actions taken to respond to such breaches. OCR will make every effort, as permitted by law, to protect information that identifies individuals or that, if released, could constitute a clearly unwarranted invasion of personal privacy.

I attest, to the best of my knowledge, that the above information is accurate.

\* Name: Carl W. Patten, Jr. Date: 11/07/2019

