

February 23, 2021

Attorney General
SecurityBreach@atg.wa.gov

RE: Case 283533

NOTICE OF PRIVACY INCIDENT

Dear Attorney General;

The purpose of this letter is to notify your office of a recent privacy incident that occurred and impacted residents of your state. First, let me state that Humana takes all privacy concerns seriously and is taking appropriate steps to prevent errors such as this in the future.

What Happened?

On December 22, 2020, Humana was informed that an employee of a Humana subcontractor inappropriately used their access to individual information to disclose information, in the form of medical records, to unauthorized individuals in an effort to train medical coders for a personal coding business endeavor. The subcontractor discovered the incident on December 16, 2020. The activity occurred October 12, 2020 through December 16, 2020. We deeply apologize for this situation.

Cotiviti is a vendor Humana uses for quality reporting and risk adjustment purposes. Risk adjustment is required of Medicare Advantage plans, like Humana, by the federal Medicare agency, the Centers for Medicare and Medicaid Services (CMS). By risk adjusting plan payments, CMS is able to make appropriate and accurate payments for enrollees with differences in expected costs. Cotiviti provides systems that allow Humana to contact health care providers and request medical records for this process.

Cotiviti utilizes a subcontractor, Visionary. A Visionary employee was attempting to train unauthorized individuals on how to conduct Medicare Risk Adjustment coding as part of a personal business endeavor. The Visionary employee, who was authorized to access and use the data for Humana purposes, disclosed the information to the unauthorized individuals through a personal Google Drive account.

Humana requires executed Business Associate Agreements with all organizations that perform any services on our behalf involving our member's protected health information. This Business Associate Agreement requires Cotiviti to comply with federal Health Insurance Portability and Accountability Act (HIPAA) privacy regulations and to follow guidelines and policies established by Humana in maintaining the privacy and confidentiality of all protected health information. We also conduct assessments of our business associates to verify that processes

are being followed. Similarly, Cotiviti has executed Business Associate Agreements with their subcontractors that holds them to these same standards

What Information Was Involved?

The following information may have been included as part of the medical records involved in the incident:

- Full Social Security Number
- Partial Social Security Number
- Name
- Date of Birth
- Address
- City
- State
- Zip Code
- Phone number
- Email address
- Member Identification Number
- Subscriber Identification Number
- Date of Service
- Date of Death
- Provider Name
- Medical Record Number
- Treatment Related Information
- Actual Images (x-ray, photographs, etc.)

What Are We Doing?

On February 25, 2021, notification letters will be sent to 675 residents of your state who were impacted by this situation. Attached you will find a copy of the letter that includes an application for free credit monitoring and free identity theft protection for two years. There is no cost to the individuals for this service.

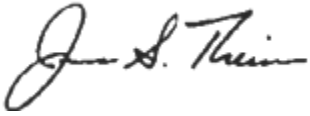
We deeply regret this incident, but want to assure you that Humana has safeguards to protect individual information including policies, procedures and technical safeguards. As a result of this incident Humana has worked with Cotiviti to ensure immediate steps were taken to enhance protections and ensure the safety and security of individual's information. To help prevent something like this from happening again, Humana has taken prompt action to ensure the appropriate physical and technical safeguards are in place at Cotiviti and Visionary.

Upon discovery, Visionary immediately disabled the access of the now former employee into Visionary and Cotiviti systems. Visionary implemented a broad containment strategy to prevent any information that was subject to unauthorized disclosure, due to this incident, from further unauthorized disclosure. Both Visionary and Cotiviti launched a comprehensive investigation into the incident and hired cybersecurity firms to assist in the efforts.

Humana will promptly report to your office and appropriate law enforcement officials any information that is shared with us that indicates this information has been inappropriately used.

Please do not hesitate to contact me if you have any additional questions regarding this situation.

Sincerely,

A handwritten signature in black ink that reads "James S. Theiss". The signature is written in a cursive style with a large initial "J" and a distinct "S".

James S. Theiss
Chief Privacy Officer
Humana Inc.
502-580-4322
jtheiss@humana.com

Enclosures

HUMANA INC
PRIVACY OFFICE
101 E MAIN STREET
LOUISVILLE KY 40202



February 25, 2021

FIRSTNAME LASTNAME
ADDR1 ADDR2
CITY STATE ZIP

RE: 283533

NOTICE OF PRIVACY INCIDENT

Equifax Activation Code: xxxxxxxxxxxxxxxx

Dear FIRSTNAME LASTNAME;

We are writing to notify you, a valued member, of a recent incident involving some of your personal information.

What Happened?

On December 22, 2020, Humana was informed that an employee of a Humana subcontractor inappropriately used their access to your information to disclose information, in the form of medical records, to unauthorized individuals in an effort to train medical coders for a personal coding business endeavor. The subcontractor discovered the incident on December 16, 2020. The activity occurred October 12, 2020 through December 16, 2020. We deeply apologize for this situation.

Cotiviti is a vendor Humana uses for quality reporting and risk adjustment purposes. Risk adjustment is required of Medicare Advantage plans, like Humana, by the federal Medicare agency, the Centers for Medicare and Medicaid Services (CMS). Cotiviti provides systems that allow Humana to contact health care providers and request medical records for this process.

Cotiviti utilizes a subcontractor, Visionary. A Visionary employee was attempting to train unauthorized individuals on how to conduct Medicare Risk Adjustment coding as part of a personal business endeavor. The Visionary employee, who was authorized to access and use the data for Humana purposes, disclosed the information to the unauthorized individuals through a personal Google Drive account.

Humana requires executed Business Associate Agreements with all organizations that perform any services on our behalf involving our members' protected health information. This Business Associate Agreement requires Cotiviti to comply with federal Health Insurance Portability and Accountability Act (HIPAA) privacy regulations and to follow guidelines and policies established by Humana in maintaining the privacy and confidentiality of all protected health information. We also conduct assessments of our business associates to verify that processes are being followed. Similarly, Cotiviti has executed Business Associate Agreements with their subcontractors that holds them to these same standards.

What Information Was Involved?

The following information may have been included as part of the medical records involved in the incident:

- Full Social Security Number
- Partial Social Security Number
- Name
- Date of Birth
- Address
- City
- State
- Zip Code
- Phone number
- Email address
- Member Identification Number
- Subscriber Identification Number
- Date of Service
- Date of Death
- Provider Name
- Medical Record Number
- Treatment Related Information
- Actual Images (x-ray, photographs, etc.)

What Are We Doing?

Humana is committed to safeguarding your personal information. Humana has worked with Cotiviti to ensure it took immediate steps to enhance protections and ensure the safety and security of your information now and into the future. To help prevent something like this from happening again, Humana has taken prompt action to ensure the appropriate physical and technical safeguards are in place at Cotiviti and Visionary.

Upon discovery, Visionary immediately disabled the access of the now former employee for both Visionary and Cotiviti systems. Visionary implemented a broad containment strategy to prevent any information that was subject to unauthorized disclosure, due to this incident, from further unauthorized disclosure. Both Visionary and Cotiviti launched a comprehensive investigation into the incident and hired cybersecurity firms to assist in the efforts.

We know that you may be worried about what took place.

To help relieve concerns and restore confidence following this incident, we have partnered with Equifax® to provide its Credit Watch™ Gold with 3-in-1 Monitoring identity theft protection product to you for two years. There is no cost for the service. A description of this product and instructions about how to enroll were included with the letter you received.

We strongly encourage you to enroll in this no cost service to protect yourself from the potential misuse of your information.

What You Can Do

We do not think your personal information will be used inappropriately because of the incident that took place. However, we ask you to remain vigilant. There are steps you can take to protect yourself. Review the following for suspicious activity:

- Explanation of Benefit (EOB) letters
- SmartSummary Statements
- Medical Records
- Account Statements and Credit Reports

Watch for services you did not receive or accounts you did not open. If you find unfamiliar activity on the statements you receive from Humana, please notify us immediately. Keep a copy of this notice in case of future problems with your medical records.

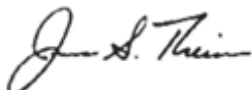
If you see suspicious activity on your credit report, call your local police office to file a report for identity theft. Get a copy of the report. Details are enclosed to obtain additional information from the Federal Trade Commission (FTC) and consumer reporting agencies. You can learn to place a fraud alert and/or security freeze on your account.

For More Information

Do you have any questions or need help with anything mentioned in this letter? Please contact us at 1-800-457-4708. If you have a speech or hearing impairment and use a TTY, call **1-800-833-3301**.

Again, please accept our sincere apology for this incident. We value your membership and work hard to protect your information.

Sincerely,



Jim Theiss
Chief Privacy Official
Humana, Inc.
Privacy Office

Enclosures

Identity Theft Guide

You are advised to report any suspected identity theft to law enforcement. You have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

In addition, the Federal Trade Commission suggests the following:

1. **Fraud Alert.** Contact the toll-free number of any of the three consumer reporting companies below to place a fraud alert on your file. You only need to contact one of the three companies to place an alert. The company you call is required to contact the other two companies. 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 delay you when you seek to obtain credit. Under federal law, you may place a fraud alert on your file free of charge.

Equifax P.O. Box 740256 Atlanta, GA 30348 1-800-685-1111 www.equifax.com	Experian P.O. Box 4500 Allen, TX 75013 1-888-EXPERIAN or 1-888-397-3742 www.experian.com	TransUnion P.O. Box 2000 Chester, PA 19016 1-800-916-8800 www.transunion.com
--	--	--

2. **Free Credit Report.** You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit-reporting agencies. To order your annual free credit report please visit www.annualcreditreport.com or call toll free at 1- 877-322-8228. Even if you do not find any signs of fraud on your credit reports, experts in identity theft recommend you check your credit reports every three months for the next year.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Services, P.O. Box 105281, Atlanta, GA 30348-5281.

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

Contact the Federal Trade Commission and your state Attorney General. If you believe you are the victim of identity theft or your personal information has been misused, you can contact the Attorney General's Office in your home state and/or the Federal Trade Commission at 1- 877-ID-THEFT, (1-877-438-4338) or by visiting the Federal Trade Commission website at

www.ftc.gov/idtheft or write Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

For residents of Maryland: You may also obtain information about identity theft prevention from the:

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

For residents of North Carolina: You may also obtain information about identity theft prevention from the:

North Carolina Attorney General's Office

Consumer Protection Division 9001 Mail Service Center Raleigh, NC 27699-9001
1-877-5-NO-SCAM, www.ncdoj.gov

For residents of Rhode Island: You may also obtain information about identity theft prevention from the:

Office of the Rhode Island Attorney General

Consumer Protection Unit 150 South Main Street
Providence, Rhode Island 02903
(401) 274-4400, consumers@riag.ri.gov

Security Freeze: You may also place a security freeze on your credit reports, free of charge. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services. Under federal law, you cannot be charged to place, lift, or remove a security freeze.

You must place your request for a freeze with each of the three major consumer reporting agencies: Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com). To place a security freeze on your credit report, you may send a written request by regular, certified or overnight mail to Equifax, Experian and TransUnion at the addresses above. You may also place a security freeze through each of the consumer reporting agencies' websites or over the phone, using the contact information above.

In order to request a security freeze, you will need to provide some or all of the following information to the credit reporting agency, depending on whether you do so online, by phone, or by mail:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;

4. If you have moved in the past five (5) years, the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill, telephone bill, rental agreement, or deed;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. Social Security Card, pay stub, or W2;
8. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have one (1) to three (3) business days after receiving your request to place a security freeze on your credit report, based upon the method of your request. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password (or both) that can be used by you to authorize the removal or lifting of the security freeze. It is important to maintain this PIN/password in a secure place, as you will need it to lift or remove the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must make a request to each of the credit reporting agencies by mail, through their website, or by phone (using the contact information above). You must provide proper identification (including name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report. You may also temporarily lift a security freeze for a specified period of time rather than for a specific entity or individual, using the same contact information above. The credit bureaus have between one (1) hour (for requests made online) and three (3) business days (for request made by mail) after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must make a request to each of the credit reporting agencies by mail, through their website, or by phone (using the contact information above). You must provide proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have between one (1) hour (for requests made online) and three (3) business days (for requests made by mail) after receiving your request to remove the security freeze.

Discrimination is against the law

Humana Inc. and its subsidiaries comply with applicable federal civil rights laws and do not discriminate on the basis of race, color, national origin, age, disability, or sex. Humana Inc. and its subsidiaries do not exclude people or treat them differently because of race, color, national origin, age, disability, or sex.

Humana Inc. and its subsidiaries provide: (1) free auxiliary aids and services, such as qualified sign language interpreters, video remote interpretation, and written information in other formats to people with disabilities when such auxiliary aids and services are necessary to ensure an equal opportunity to participate; and, (2) free language services to people whose primary language is not English when those services are necessary to provide meaningful access, such as translated documents or oral interpretation.

If you need these services, call **1-877-320-1235** or if you use a **TTY**, call **711**.

If you believe that Humana Inc. and its subsidiaries have failed to provide these services or discriminated in another way on the basis of race, color, national origin, age, disability, or sex, you can file a grievance with Discrimination Grievances, P.O. Box 14618, Lexington, KY 40512-4618.

If you need help filing a grievance, call **1-877-320-1235** or if you use a **TTY**, call **711**.

You can also file a civil rights complaint with the **U.S. Department of Health and Human Services**, Office for Civil Rights electronically through the Office for Civil Rights Complaint Portal, available at <https://ocrportal.hhs.gov/ocr/portal/lobby.jsf>, or by mail or phone at **U.S. Department of Health and Human Services**, 200 Independence Avenue, SW, Room 509F, HHH Building, Washington, DC 20201, **1-800-368-1019, 800-537-7697 (TDD)**.

Complaint forms are available at <https://www.hhs.gov/ocr/office/file/index.html>

Multi-Language Interpreter Services

ATTENTION: If you do not speak English, language assistance services, free of charge, are available to you. Call **1-877-320-1235 (TTY: 711)**.... ATENCIÓN: si habla español, tiene a su disposición servicios gratuitos de asistencia lingüística. Llame al **1-877-320-1235 (TTY: 711)**.... 注意: 如果您使用繁體中文, 您可以免費獲得語言 援助服務。請致電 **1-877-320-1235 (TTY: 711)**。... CHÚ Ý: Nếu bạn nói Tiếng Việt, có các dịch vụ hỗ trợ ngôn ngữ miễn phí dành cho bạn. Gọi số **1-877-320-1235 (TTY: 711)**.... 주의: 한국어를 사용하시는 경우, 언어 지원 서비스를 무료로 이용하실 수 있습니다. **1-877-320-1235 (TTY: 711)**번으로 전화해 주십시오.... PAUNAWA: Kung nagsasalita ka ng Tagalog, maaari kang gumamit ng mga serbisyo ng tulong sa wika nang walang bayad. Tumawag sa **1-877-320-1235 (TTY: 711)**.... Если вы говорите на русском языке, то вам доступны бесплатные услуги перевода. Звоните **1-877-320-1235 (телефайп: 711)**.... ATANSYON: Si w pale Kreyòl Ayisyen, gen sèvis èd pou lang ki disponib gratis pou ou. Rele **1-877-320-1235 (TTY: 711)**.... ATTENTION : Si vous parlez français, des services d'aide linguistique vous sont proposés gratuitement. Appelez le **1-877-320-1235 (ATS: 711)**.... UWAGA: Jeżeli mówisz po polsku, możesz skorzystać z bezpłatnej pomocy językowej. Zadzwoń pod numer **1-877-320-1235 (TTY: 711)**.... ATENÇÃO: Se fala português, encontram-se disponíveis serviços linguísticos, grátis. Ligue para **1-877-320-1235 (TTY: 711)**.... ATTENZIONE: In caso la lingua parlata sia l'italiano, sono disponibili servizi di assistenza linguistica gratuiti. Chiamare il numero **1-877-320-1235 (TTY: 711)**... ACHTUNG: Wenn Sie Deutsch sprechen, stehen Ihnen kostenlos sprachliche Hilfsdienstleistungen zur Verfügung. Rufnummer: **1-877-320-1235 (TTY: 711)**.... 注意事項: 日本語を話される場合、無料の言語支援をご利用いただけます。 **1-877-320-1235 (TTY: 711)**まで、お電話にてご連絡ください。... هجوت: رگا هب نابز يسراف وگتفگ يم دينك، تلايهست ي نابز تروصب ناگيار يارب امش مهارف يم دشاب. اب ... سامت دير يگب. **1-877-320-1235 (TTY: 711)**... 1-877-320-1235 (TTY: 711) ... 711. نظر حلم: اذ انتك تدهنت ركنا ءغلا، ناب تامدخ ءءعاسلا ءيو غلا رفارنت كل ناجملا ب. لصتا مقرب **1-877-320-1235 (TTY: 711)**.... 1-877-320-1235 (TTY: 711) ... مقرب فناه مصلا

GCHJV5REN 0117



About the Equifax Credit Watch™ Gold with 3-in-1 Monitoring identity theft protection product

Equifax Credit Watch will provide you with an “early warning system” to changes to your credit file and help you to understand the content of your credit file at the three major credit-reporting agencies. Note: You must be over age 18 with a credit file in order to take advantage of the product.

Equifax Credit Watch provides you with the following key features and benefits:

- Comprehensive credit file monitoring and automated alerts of key changes to your **Equifax, Experian, and TransUnion** credit reports
- Wireless alerts and customizable alerts available (available online only)
- One 3-in-1 Credit Report and access to your Equifax Credit Report™
- Up to \$1 million in identity theft insurance ¹ with \$0 deductible, at no additional cost to you
- 24 by 7 live agent Customer Service to assist you in understanding the content of your Equifax credit information, to provide personalized identity theft victim assistance and in initiating an investigation of inaccurate information.
- 90 day Fraud Alert ² placement with automatic renewal functionality* (available online only)

How to Enroll: You can sign up online or over the phone

To sign up online for **online delivery** go to www.myservices.equifax.com/tri

1. **Welcome Page:** Enter the Activation Code provided at the top of this page in the “Activation Code” box and click the “Submit” button.
2. **Register:** Complete the form with your contact information (name, gender, home address, date of birth, Social Security Number and telephone number) and click the “Continue” button.
3. **Create Account:** Complete the form with your email address, create a User Name and Password, check the box to accept the Terms of Use and click the “Continue” button.
4. **Verify ID:** The system will then ask you up to four security questions to verify your identity. Please answer the questions and click the “Submit Order” button.
5. **Order Confirmation:** This page shows you your completed enrollment. Please click the “View My Product” button to access the product features.

To sign up for **US Mail delivery**, dial 1-866-937-8432 for access to the Equifax Credit Watch automated enrollment process. Note that all credit reports and alerts will be sent to you via US Mail only.

1. **Activation Code:** You will be asked to enter your enrollment code as provided at the top of this letter.
2. **Customer Information:** You will be asked to enter your home telephone number, home address, name, date of birth and Social Security Number.
3. **Permissible Purpose:** You will be asked to provide Equifax with your permission to access your credit file and to monitor your file. Without your agreement, Equifax cannot process your enrollment.
4. **Order Confirmation:** Equifax will provide a confirmation number with an explanation that you will receive your Fulfillment Kit via the US Mail (when Equifax is able to verify your identity) or a Customer Care letter with further instructions (if your identity can not be verified using the information provided). Please allow up to 10 business days to receive this information.

Directions for placing a Fraud Alert

A fraud alert is a consumer statement added to your credit report. This statement alerts creditors of possible fraudulent activity within your report as well as requests that they contact you prior to establishing any accounts in your name. Once the fraud alert is added to your credit report, all creditors should contact you prior to establishing any account in your name. To place a fraud alert on your credit file, visit:

www.fraudalerts.equifax.com or you may contact the Equifax auto fraud line at 1-877-478-7625, and follow the simple prompts. Once the fraud alert has been placed with Equifax, a notification will be sent to the other two credit reporting agencies, Experian and Trans Union, on your behalf.

1 - Identity Theft Insurance underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.. This product is not intended for minors (under 18 years of age)

2 - The Automatic Fraud Alert feature made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC

GCHJV5REN 0117