HUMANA INC
PRIVACY OFFICE
101 E MAIN STREET
LOUISVILLE KY 40202

Humana

July 30, 2026

RECEIVED
AUG 12 2026
CONSUMER PROTECTION DIVISION

Office of the Attorney General
700 W. Jefferson Street, Suite 210
P.O. Box 83720
Boise, Idaho 83720-0010

000003 2/20

RE: Case # 1277144

NOTICE OF DATA BREACH

Dear Attorney General,

The purpose of this letter is to notify your department of a recent security incident, pursuant to our Business Associate agreement, that occurred impacting 26 Humana members that reside in 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.

DentaQuest, LLC ("DentaQuest"), a dental and vision benefits provider for certain current and former Humana Medicaid and Dual Eligible Special Needs (D-SNP) plans. DentaQuest became aware of an unauthorized third party ("Threat Actor") claiming to be in possession of data allegedly originating from its IT environment on May 20, 2026. Humana learned that residents of your State were impacted by this incident on July 20, 2026.

What Happened?

The DentaQuest business, IT, and legal teams evaluated the situation and then engaged outside legal counsel and then retained CrowdStrike Services ("CrowdStrike") to conduct an independent investigation to assess the nature, scope, and extent of Threat Actor activity within the DentaQuest environment.

CrowdStrike confirmed unauthorized access to the DentaQuest environment occurred as a result of a social engineering attack targeting a single employee account. CrowdStrike's investigation has identified that the earliest evidence of Threat Actor activity in the DentaQuest environment occurred on May 17, 2026. At that time, the Threat Actor authenticated to DentaQuest's single sign-on (SSO) environment using credentials associated with the Impacted Account, with multifactor authentication (MFA) requirements satisfied through means consistent with the social engineering attack. CrowdStrike has not identified evidence of malware or ransomware deployment, privilege escalation, or additional persistence mechanisms established within the DentaQuest environment during the period of Threat Actor activity.

CrowdStrike has not identified evidence of Threat Actor access to the DentaQuest environment since May 19, 2026. DentaQuest implemented containment measures on May 20, 2026, and monitoring of the DentaQuest environment since that date has not identified evidence of further Threat Actor activity.

What Information Was Involved?

The data is known to include the following personal and dental or vision health information: name, address, member identification number, Medicaid number, Medicare number and dental or vision health information, including provider name, diagnosis treatment and billing information. In some instances, Social Security Number was included.

What We Are Doing

DentaQuest takes this incident and the security of information within their care very seriously. DentaQuestimmediately engaged legal counsel and launched an in-depth investigation upon discovery of this incident to determine the full nature and scope. The following measures were completed:

- Revoked all SSO sessions associated with the Impacted Account.
- Deactivated the Impacted Account and rotated associated credentials.
- Disabled application-specific access associated with the Impacted Account.

Notification letters are being sent to 26 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 by Kroll. Humana and/ or DentaQuest have also notified any applicable consumer reporting agencies and any other required agency.

DentaQuest encouraged individuals to remain vigilant against incidents of identity theft and fraud by reviewing account statements and monitoring free credit reports for suspicious activity and to detect errors. The notification letter included Kroll Identity Monitoring, Fraud Consultation and Identity Theft Restoration. It provided additional details on how to take steps to protect information, should an individual feel it is necessary to do so.

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,

Privacy Office
Humana Inc.
privacyoffice@humana.com

Attachments

Privileged & Confidential

Adult Notification Template

Draft, July 7, 2026, 7 p.m.

DENTAQUEST LOGO HERE

000003 3/20

<<MemberFirstName>> <<MemberLastName>>

<<Address1>>

<<Address2>>

<<City>>, <<State>> <<Zip Code>>

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

Notice of Data Breach

Dear <<MemberFirstName>> <<MemberLastName>>,

DentaQuest works with your health plan to provide your dental or vision benefits. We are writing to tell you about a data security incident. Your personal information was accessed by unauthorized individuals. The safety of your information is very important to us. We are writing to tell you what happened and what you can do.

What happened?

On May 20, 2026, DentaQuest discovered that unauthorized individuals accessed certain data on our computer network. This included personal identification and dental or vision health information. We took immediate action to secure the network. We also reported the incident to law enforcement. We later learned that the incident began on May 17, 2026, and ended by May 20, 2026. We immediately began an investigation with leading, independent cybersecurity experts to learn what information was accessed. After finishing our review, we determined that your personal information was accessed and posted on the internet.

What information was involved?

The information included your name, <<Address, Social Security Number, Member ID number, Medicaid number, Medicare number>> and Dental or Vision Health Information, such as provider names, diagnoses, treatments and billing information.

What we are doing.

We are offering you identity theft monitoring by Kroll at no cost to you for 24 months. To try and prevent this from happening again, we engaged cyber security experts and provided more employee training. We also added new security measures and increased monitoring.

Kroll is an expert at helping people whose private data has been exposed. The identity monitoring services include Credit Monitoring, Fraud Consultation and Identity Theft Restoration. To start your identity monitoring services, visit **Enroll.krollmonitoring.com/redeem**.

You will need your Activation Code: **<<Member ID>>** and Your Verification ID: **<<Enter Verification ID>>** to enroll.

You have 90 days from the date this letter was mailed to start your identity monitoring services.

For more information about Kroll and your identity monitoring services, you can visit info.krollmonitoring.com or call 1-XXX=XXX-XXXX.

What you can do.

Please read the "Additional Resources" at the end of this letter. It describes more steps you can take to help protect yourself. This includes tips from the Federal Trade Commission about identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

For more information.

If you have questions, please call 1-XXX-XXX-XXXX, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. Please have your activation code ready.

Sincerely,

DentaQuest

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-888-4213

000003 4/20

Free Credit Report. It is recommended that you remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft. 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.**

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 Service, P.O. Box 105281, Atlanta, GA 30348-5281.

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).

Fraud Alerts. There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Security Freeze. You have the ability to place a security freeze, also known as a credit freeze, on your credit report free of charge.

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 may use an online process, an automated telephone line, or submit a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that, if you are requesting a credit report for your spouse, 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 5 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, and display your name, current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for further information on how to prevent or minimize the risks of identity theft and for additional information on fraud alerts and security freezes.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania

Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For District of Columbia residents: You may contact the Office of the District of Columbia Attorney General, 400 6th Street NW, Washington, D.C. 20001, 1-202-727-3400, www.oag.dc.gov.

For Connecticut residents: You may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

For Indiana residents: You may contact the Indiana Office of the Attorney General, Consumer Protection Division, 302 W. Washington Street, 5th Floor, Indianapolis, IN 46204, 1-800-382-5516, www.in.gov/attorneygeneral.

For Iowa residents: The Attorney General can be contacted at the Office of Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, Iowa 50319; 1-515-281-5164, www.iowaattorneygeneral.gov. You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202. , 1-888-743-0023, www.marylandattorneygeneral.gov.

For Massachusetts residents: You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html. You have the right to obtain any police report filed in connection with the cybersecurity event. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For Minnesota residents: You may contact the Minnesota Office of the Attorney General, 445 Minnesota Street, Suite 600, St. Paul, MN 55101, 1-800-657-3787, www.ag.state.mn.us.

New Mexico residents: You have rights under the federal Fair Credit Reporting Act (FCRA), which governs the collection and use of information pertaining to you by consumer reporting agencies. For more information about your rights under the FCRA, please visit www.ftc.gov.

For New York residents: The Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, www.ag.ny.gov.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226, www.ncdoj.gov.

For Oregon residents: The Attorney General can be contacted at Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096; 1-877-877-9392 (toll-free in Oregon), 1-503-378-4400, or www.doj.state.or.us. You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

For Rhode Island residents: You may contact the Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov. You have the right to file or obtain a police report regarding this incident.

KROLL

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. 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.

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.

8149100.1

Privacy Policy Summary

Protect Yourself.
Protect Humana.

Humana

**This document is a summary of general concepts of the HIPAA Privacy Rule and provides an overview of Humana's Enterprise Privacy Policies and Standards, located on Policy Source.

Note: This document was formally titled *Privacy Policy – Confidentiality of Individual Information*

Enterprise Policy Management Louisville, Kentucky

January 2025

Humana.

Dear Associate:

Humana's long-standing commitment to safeguard the privacy of our customer's information is essential to our strategy to become a consumer-focused health company. Protecting our customer's information as if it were our own has always been an integral part of how we conduct our business. It takes the commitment of all Humana associates to achieve this goal.

Attached is a summary of the enterprise privacy policies and standards located on Policy Source. The policies, standards and this summary provides Humana's intent for privacy compliance with the current regulations of the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), and with related state and federal regulations. The exception is Humana Government Business which has policies that meet the requirements of the contract held with the federal government.

The Privacy Office is responsible for the development, maintenance, and implementation of all enterprise policies and standards. The enterprise privacy policies and standards will be reviewed annually, and revisions will be made as necessary to remain current with new legislation. Any questions or concerns should be referred to the Privacy Office via e-mail: privacyoffice@humana.com.

Please join us in our continued commitment to build a more informed workforce that is committed to a knowledgeable, privacy-compliant environment.

Sincerely,

James S. Theiss
Associate VP, Privacy & Ethics

Table of Contents

Preface

About this Document

This *Privacy Policy Summary* is sponsored by the Humana Privacy Office. This is a summary of key elements of the Privacy Rule and our enterprise privacy policies and standards, located on Policy Source. This document is not a complete or comprehensive guide to compliance. Humana is an entity regulated by the Privacy Rule and state privacy laws. We are obligated to comply with all its applicable requirements and should not rely on this summary. In the event of a conflict between this summary and the enterprise-wide privacy policies and standards, the policies and standards govern.

Distribution

Associates may view an online version of this document through HI! on Policy Source (go/policysource – Enterprise Risk and Compliance (ER&C) – Compliance – Privacy and Ethics – Privacy – Privacy Policy Summary).

This document is written as an online reference document. It is designed to be read on HI!. For short-term reference needs, as required, associates may print paper copies of pages in this document. However, the online document is the source document. Associates should refer to the most current document at the website. Print versions are uncontrolled, and as such, become outdated each time a revision or new edition is published on HI!.

Comments

If you would like to make any comments regarding this document, please go to the Privacy Office e-mail at privacyoffice@humana.com. All comments help provide needed information for future revisions.

Interpretations and Variation Summary

This document is intended as a guideline. Situations may arise in which professional judgment may necessitate action that differs from the guidelines in this document. An explanation of the special circumstances that justify the variation from the guidelines should be documented and retained in the file/record.

Questions about concepts or guidelines in the document should be referred to the Privacy Office. Prior to making an exception, a written request should be made to and approved in writing by the Privacy Office. Send an e-mail to the Privacy Office at privacyoffice@humana.com.

Summary of Changes:

- Updated the month on page 2

Introduction to the Privacy Policy Summary

Focus

The enterprise privacy policies and standards and this summary provide guidelines which should be followed by all Humana Inc. operating entities, subsidiaries, affiliates, business groups, markets and/or departments. It applies to all Humana associates, and all temporarily assigned individuals, all contractors, vendors, or others who are provided with authorized access to Humana's Information Technology Systems or the information derived from those systems ("User"). The privacy policies and this summary apply to oral, written, and electronic individually identifiable health information and non-public personal information in all Humana facilities and operational areas (referred to as "Humana" throughout this document). The information protected applies to individual, member, patient, agent, broker, employer group, provider, vendors and third parties including person(s) who are deceased. The protection still applies in the event Humana no longer does business.

Humana will follow all Federal and state laws and regulations. Where more than one state is impacted by a particular issue, to allow for consistency, Humana will follow the most stringent requirement.

Privacy Office

The role of Humana's Privacy Office is to oversee activities related to the development, implementation, maintenance of, and compliance to the organization's privacy policies, standards, and procedures for protected information. The Privacy Office responsibilities also include, but are not limited to, the following:

- Monitoring and assessing Humana's Privacy Program
- Development and review of privacy notices for compliance with federal and state law
- Reviewing and responding to potential privacy violations, privacy incidents and/or breaches
- Managing the Protected Health Information and Vendor Ethics (PHIVE) committee
- Providing privacy consultation and support to all Humana departments
- Providing privacy education and awareness

The Privacy Office maintains a web site at go/privacy for all associates to access and use for privacy-related issues, or associates may contact the Privacy Office via:

- E-mail: privacyoffice@humana.com
- Fax: (502) 508-3700
- U.S. Mail: Humana Inc.
  Privacy Office 003/10911
  101 E. Main Street
  Louisville, KY 40201

Compliance with Federal and State Privacy Laws

In accordance with Federal and state privacy laws, Humana has fulfilled several administrative requirements to demonstrate compliance. Listed below are some of those requirements, with a brief description:

- Humana has appointed a Privacy Official. The role of the Privacy Official is to be the central point of contact for all privacy-related issues in Humana.
- The Privacy Office has developed and implemented the enterprise privacy policies and standards. The policies and standards are revised as necessary by the Privacy Office and reviewed and approved annually. The privacy policies and standards support, and are

compliant with, state and federal privacy regulations. Business areas throughout Humana are expected to develop departmental policies and procedures that reflect compliance with enterprise privacy policies.

- Newly hired associates and newly assigned contingent labor are required to complete the training within 30 days of start date. This training must be completed prior to receiving access to view or manipulate Protected Health Information (PHI) either in a training or operational setting.
- Humana has developed and implemented safeguards to protect information that includes administrative, technical, and physical elements.
- Humana does not use or disclose protected health information for employment-related actions and decisions or in connection with any other benefit or employee benefit plan without authorization.
- Humana has developed policies and standards to apply appropriate sanctions to associates who fail to comply with the privacy policies. The Privacy Office works in coordination with the appropriate Human Resources Department to enforce the privacy policies and, in the event of privacy violations, to assist in determining disciplinary actions.
- The Privacy Office is responsible for handling privacy-related complaints.
- Humana will mitigate to the extent practical, any known harmful effect of any violation of privacy policies and standards, including any violations of our business associates.
- Humana will not intimidate, threaten, coerce, discriminate against, or take other retaliatory actions against individuals exercising their individual rights, or anyone filing a complaint, or participating in an investigation or compliance review.

Humana does not require individuals to waive their right to file a complaint with the Office of Civil Rights to continue to receive health care benefits.

Individual Privacy Rights

Individual Privacy Rights

HIPAA provides individuals with various options we refer to as individual rights. Individual privacy rights may be invoked by the individual or, if appropriate information is provided, by authorized personal representative(s). The following are brief descriptions of the various individual rights.

Privacy Notice

As Humana continues to expand products and services, the Privacy Office has developed different Notices of Privacy Practices to meet those needs. Individuals have the right to receive and request a *Notice of Privacy Practices*. This notice describes the uses and disclosures of protected information, provides an explanation of individual privacy rights, and outlines how to file a privacy complaint. Humana distributes the Notice of Privacy Practices in accordance with applicable federal and state laws, rules, and regulations.

Access

The right to request access to protected health information allows individuals the opportunity to review and/or obtain a photocopy (or other such format including electronic) of their information maintained by Humana. Humana responds in accordance with federal and state law and will follow the most stringent requirement.

The default process for communicating PHI in response to an access request should always be in a secure manner. If an individual requests information be sent in an "unsecure" manner such as via standard email, they must be advised of the potential risk. If the individual indicates they still prefer the manner requested, the information can be sent and the transaction, (individual request and advisement of potential risk) should be documented appropriately.

It is Humana's practice to provide individuals or their personal representatives' access to their information free of charge; however, Humana may impose a reasonable, cost-based fee if an individual or their personal representative requests a copy of their PHI (or agrees to receive a summary or explanation of the information.) Below are the options for charging:

- The fee may be a flat fee not to exceed $6.50 for entities that do not want to go through the process of calculating actual or average costs as described below.
- Calculation by using a schedule of costs based on average allowable labor costs to fulfill standard requests.
- Fee calculation of actual allowable costs to fulfill each request to include only the cost of:
    1. Labor for copying the PHI requested by the individual, whether in paper or electronic form. Labor may include preparation of an explanation or summary of the PHI, if summary format is agreed by the individual in advance.
    2. Supplies for creating the paper copy or electronic media (e.g., CD or USB drive) if the individual requests that the electronic copy be provided on portable media.
    3. Postage, when the individual requests the copy, or the summary or explanation, to be mailed.

The fee may not include costs associated with verification; documentation; searching for and retrieving the PHI; maintaining systems; recouping capital for data access, storage, or infrastructure; or other costs not listed above even if such costs are authorized by State law.

Contact the Privacy Office for guidance if your area is considering charging individuals or their personal representatives for access to their records.

Accounting

The right to an accounting allows individuals to request a list of disclosures of their protected health information made by Humana or our business associates for purposes other than treatment, payment, health plan operations, and other activities in the past six years. Some activities Humana is required to account for include, but are not limited to, audits by health oversight agencies for audit, investigations, licensure, for judicial and administrative proceedings (court order, subpoena, discovery, etc.), and for research purposes.

Restriction

The right to restrict allows individuals to request a limit or restriction on the use and disclosure of their protected health information. Humana is not required to agree to the restriction if it is determined that the restriction may interfere with treatment, payment, or operations. If approved, Humana abides by the restriction, except in emergencies and as required by law.

Pay Out of Pocket

In addition, an individual or their representative may advise their service provider (i.e., Physician) of their intention to pay in full out of pocket for a service and request the services not be sent to their health plan carrier. In this instance, where an individual pays for a health care item or service out of pocket in full, inclusion of information related to the transaction/s is restricted.

Restriction Termination

The right to remove a restriction allows individuals the ability to request or agree to the removal of a previously requested restriction.

Alternate Communications

The right to ask that we send health information to a member or patient at a different address or by a different communication method (such as email). This individual privacy right may be exercised in life threatening situations.

**Note: If such a request is urgent, please notify the Privacy Office immediately and we will attempt to accommodate verbal requests with the understanding that the request will be followed up in writing.

Amendment

The right to amend allows individuals the right to request a correction of their protected health information created and maintained by Humana that is inaccurate and/or incomplete. Upon receipt of a written request, the Privacy Office responds within sixty (60) days unless an extension is needed. The Privacy Office may deny the request. If the Privacy Office denies a request, a written explanation is provided to the individual.

File a Complaint

The right to file a complaint allows individuals the opportunity to express, to Humana or the Secretary of the Department of Health and Human Services, any concerns of dissatisfaction regarding privacy issues. The Privacy Office conducts, in a timely manner, a thorough and impartial investigation of any complaints filed by individuals who believe that their protected health information has been collected, used, accessed, disseminated, or transmitted improperly. The Privacy Office documents all complaints received and the outcomes of the investigation.

Humana will not intimidate, threaten, coerce, or take retaliation against any individuals for exercising their individual rights, or for participating in any process established by the privacy regulations including filing a complaint with Humana or the Secretary of the Department of Health and Human Services.

Contact the Privacy Office for information on how to file a complaint with the Secretary of the Department of Health and Human Services.

The Privacy Office documents and maintains requests for a minimum of six (6) years, or longer, in compliance with the current *Records Retention Program*. See also the records retention schedule on the *Records Management Portal*.

Gramm-Leach-Bliley Act (GLBA)

While Humana's *Privacy Policy and this Summary* provide guidelines for compliance with HIPAA, they also provide guidelines for privacy compliance with other federal and state privacy regulations, such as the Gramm-Leach-Bliley Act (GLBA). HIPAA Privacy and GLBA Privacy are complimentary in that they work together to achieve the goal of protecting individually identifiable health (HIPAA Privacy), and individually identifiable financial and non-public personal (GLBA) information. Examples of financial information include, but are not limited to, an individual's bank account number and premium payment history. Non-public personal information could include, but is not limited to, consumers name, address, telephone number, date of birth, social security number, and any other information that was derived from any type of application or form.

Similar to HIPAA, GLBA requires Humana to provide a written notice to individuals that explains its privacy policies in regard to individually identifiable financial and non-public personal information. Government programs such as Medicare and Medicaid are excluded from this regulation. In addition, this regulation requires Humana to inform individuals that Humana may release "non-public personal information" to affiliated companies, and nonaffiliated third parties—as permitted by law.

Humana may also provide non-public personal information to other financial institutions with which Humana has joint marketing agreements in order to provide Humana members/patients with offers for products and services they may find of value, and which are not products offered by Humana, again, unless the individual denies permission by "opting out."

Uses & Disclosures of Protected Health Information

Required Disclosures

Humana is required by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) to disclose protected health information to an individual who is the subject of the information and to the Department of Health and Human Services to determine compliance with the regulations.

Permitted Uses and Disclosures without Authorization

Humana is permitted, but not required, to use and/or disclose protected health information without authorization for the following purposes or situations:

a) For treatment, payment, and health plan operations
b) For public interest and benefit activities
c) For financial reporting and processing purposes
d) If it is incidental to an otherwise permitted use and disclosure.
e) To another covered entity or a health care provider for the payment activities of the entity that receives the information that participates in an organized health care arrangement. The entity may disclose protected health information about an individual to other participants in the organized health care arrangement for any health care operations activities of the organized health care arrangement.
f) While Humana does not participate in an organized health care arrangement, a covered entity that participates in an organized health care arrangement may disclose protected health information about an individual to other participants in the organized health care arrangement for any health care operations activities of the organized health care arrangement.

a) Treatment, Payment, and Health Plan Operations

Humana, the health plan may use and/or disclose protected health information to a doctor, a hospital or other covered entity for the individual to receive medical treatment, to pay claims for covered services provided to the individual by physicians, hospitals, or other entities. Humana owned providers may use and/or disclose protected health information to a doctor, a hospital or other entity for submission of patient claims for payment, communicating patient treatment plans, securing medical equipment or facility space, therapy, or other related support services. In addition, both Humana health plan and owned providers may use health information to conduct some of the activities as listed below, based on their role.

- Accreditation and Credentialing: Humana Health Plan and Humana owned providers may use and/or disclose protected health information to review the competency or qualifications of health care professionals, evaluating health plan performance, accreditation, certification, licensing, or credentialing activities.
- Business Management: Humana may use and/or disclose protected health information for business planning such as facility growth, acquiring equipment for patient medical procedures, conducting cost management, and planning related analysis, including formulary development and administration, improvement to methods of payment or claims submission methods, purchasing patient management software and conducting due diligence in connection with the purchase, sale, or transfer of assets.
- Compliance Programs and Health Oversight Activities: Humana Health Plan and Humana owned providers may use and/or disclose protected health information for audit functions and oversight activities, including those authorized by law. These activities may include, but are not limited to, the following: fraud and abuse detection, compliance programs, patient health improvement activities, inspections, licensure, or disciplinary actions and legal services.

- Coordination of Benefits: Humana may use and/or disclose protected health information for collection from or disclosure to another carrier when receiving the information to investigate, evaluate, adjust, or settle a claim(s) involving the subject of the protected health information.
- Customer Service Activities: Humana Health Plan and Humana owned providers may use and/or disclose protected health information for performing customer service, resolution of internal grievances, and conducting medical reviews.
- Disease Management: Humana Health Plan and Humana owned providers may use and/or disclose protected health information to identify patient populations with acute and/or chronic diseases or conditions requiring and/or introducing interventions (education, compliance with appropriate recommended therapies with drugs, and/or procedures, prevention and/or maintenance).
- Health and Wellness Information: Humana Health Plan and Humana owned providers may use and/or disclose protected health information to provide information about health-related benefits and services, appointment reminders, or about treatment alternatives.
- Plan Sponsors/Benefit Administrators: Humana Health Plan may use and/or disclose protected health information as appropriate to support the plan sponsor/benefit administrator in performing plan administration functions.
- Quality and Utilization Management: Humana Health Plan and Humana owned providers may use and/or disclose protected health information to conduct quality investigations, quality improvement projects, outcome evaluations, development of clinical guidelines, population-based activities, services coordination, case management, and other utilization management activities.
- Subrogation: Humana may use and/or disclose protected health information to investigate, evaluate, subrogate, or settle third-party claims.
- Training: Humana Health Plan and Humana owned providers may use and/or disclose protected health information to conduct training programs in which students, trainees, or practitioners in areas of heath care learn under supervision to practice or improve their skills as health care providers. In these situations, contact the Privacy Office for guidance on the appropriate safeguards that should be in place for these situations.
- Underwriting: Humana Health Plan may use and/or disclose protected health information for underwriting, premium rating, reinsurance activities, or other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits.

Note: If Humana receives protected health information for underwriting, premium rating, reinsurance activities or other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits and is not selected as the plan by the plan member, Humana may not use and/or disclose such information for any other purpose except as required by law.

b) For Public Interest and Benefit Activities

Humana Health Plan and Humana owned providers may use and/or disclose protected health information for public interest and benefit activities without authorization from the individual in the following situations. For any of the situations below, unless otherwise specified, please contact the Privacy Office for guidance.

- Required by Law: Humana Health Plan and Humana owned providers may use and/or disclose protected health information when we are required to do so by law including federal, tribal, state, or local.
- Public Health and Safety: Humana Health Plan and Humana owned providers may use and/or disclose protected health information to public health authorities and their authorized agents for public health purposes including but not limited to public health surveillance, investigations, situations involving domestic violence, and interventions.

- Research: Humana Health Plan and Humana owned providers may use and/or disclose protected health information for clinical research purposes without authorizations in limited circumstances upon approval from the PHIVE Committee. Refer to the Guidelines for Uses & Disclosures of Protected Health Information section for additional details regarding the PHIVE Committee.
- Abuse, Neglect or Domestic Violence: Humana Health Plan and Humana owned providers may use and/or disclose protected health information to report abuse, neglect, or domestic violence under specified circumstances.
- Law Enforcement: Humana Health Plan and Humana owned providers may use and/or disclose protected health information to law enforcement officials for law enforcement purposes under certain circumstances and subject to specified conditions including to help identify and locate a suspect, fugitive, or missing person; as required by law and administrative requests; in response to a law enforcement official's requests for information about a victim or suspected victim of a crime; to alert law enforcement of a person's death if the covered entity suspects that criminal activity caused the death; and to provide information related to a crime that occurred on Humana premises.
- Judicial and Administrative Proceedings: Humana Health Plan and Humana owned providers may use and/or disclose protected health information in the course of a judicial or administrative proceeding under specified circumstances. *Consult with the appropriate Critical Inquiry Department and/or Risk Manager for your area prior to disclosure.*
- Organ Donation: Humana Health Plan and Humana owned providers may use and/or disclose protected health information for procurement, banking, or transplantation of organs, eyes, or tissues.
- Compliance Programs and Health Oversight Activities: Humana Health Plan and Humana owned providers may use and/or disclose protected health information for audit functions and oversight activities, including those authorized by law. These activities may include, but are not limited to, the following: fraud and abuse detection, compliance programs, inspections, licensure, or disciplinary actions and legal services. *Consult with the Compliance, Privacy Office, or Law Department for assistance.*
- Worker's Compensation: Humana Health Plan and Humana owned providers may use and/or disclose protected health information where necessary to fulfill Humana's obligations under any workers' compensation law or contract.
- Death: Humana Health Plan and Humana owned providers may use and/or disclose protected health information of a deceased individual to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law. Humana may disclose protected health information to a funeral director, consistent with applicable law, as necessary to carry out their duties with respect to the decedent.
- Serious Threat to Health or Safety: Humana Health Plan and Humana owned providers may use and/or disclose protected health information that we deem necessary to prevent or lessen a serious and imminent threat to a person or the public, when such use and/or disclosure is made to someone they believe can prevent or lessen the threat.
- Specialized Government Functions: Humana Health Plan and Humana owned providers may use and/or disclose protected health information for specialized government functions including but not limited to determining eligibility for or conducting enrollment in certain government benefit programs and conducting intelligence and national security activities that are authorized by law.
- National Instant Criminal Background Check System (NICS) Humana may use or disclose protected health information for purposes of reporting to the National Instant Criminal Background Check System the identity of an individual who is prohibited from possessing a firearm under the law. Humana may disclose to the NICS the identities of individuals who are

subject to a Federal "mental health prohibitor" that disqualifies them from shipping, transporting, possessing, or receiving a firearm. This applies to providers who make determinations that disqualify individuals from having a firearm or who are designated by their State to report the information. Humana must:

- Disclose the information only to:
  - The National Instant Criminal Background Check System; or
  - An entity designated by the State to report, or which collects information for purposes of reporting, on behalf of the State, to the National Instant Criminal Background Check System; and
  - Discloses only the limited demographic and certain other information (name, date of birth, sex, who submitted it and supporting documentation) needed for purposes of reporting to the National Instant Criminal Background Check System; and
  - Does not disclose diagnostic or clinical information for such purposes.

- Food and Drug Administration: Humana Health Plan and Humana owned providers may use and disclose to the Food and Drug Administration (FDA) protected health information relative to adverse events with respect to drugs, foods, supplements, products, and product defects, or post marketing surveillance information to enable product recalls, repairs, or replacement.

c) Financial Reporting and Purposes
Humana Health Plan and Humana owned providers may use and/or disclose protected health information for banking and payment processes, such as to financial institutions or entities acting for financial institutions, if necessary for processing payments for health care treatment services and health plan premiums.

d) Incidental to an Otherwise Permitted Use and Disclosure
The use or disclosure of protected health information that occurs because of an otherwise permitted use or disclosure is acceptable if Humana has implemented both reasonable safeguards and implemented the minimum necessary standard as required by the Privacy Rule.

Opportunity for the Individual to Agree or Object

Humana Health Plan and Humana owned providers may use and/or disclose protected health information in some situations provided that the individual is informed in advance of the use or disclosure and has the opportunity to agree to or prohibit or restrict the use or disclosure.

- Disaster Relief: Humana Health Plan and Humana owned providers may use and/or disclose protected health information to a public or private entity authorized by law or by its charter to assist in disaster relief efforts. The purpose of the use and/or disclosure with such entities is to notify or assist in the notification of (including identifying or locating), a family member, a personal representative of the individual or another person responsible for the care of the individual of the individual's location, general condition, or death.
- Individual's Care and Payment: Humana Health Plan and Humana owned providers may use and/or disclose protected health information to a family member, other relative or a close personal friend of the individual or any other person identified by the individual the protected health information directly relevant to the person's involvement with the individual's care or payment related to the individual's health care.
- Emergency Situations: In emergency situations when the individual is not present or is incapacitated, Humana Health Plan and Humana owned providers may use their professional judgment to determine if it is in the best interest of the individual to use and/or disclose the information. In these situations, disclose only the protected health information that is directly relevant to the person's involvement with the individual's health care.

- Reproductive Health Care: For any disclosure relating to reproductive health care information, an attestation that the purpose of the request is not for a prohibited purpose from the requestor must be obtained prior to the release of such information. Please work with the Privacy Office and Law department to understand additional obligations of safeguarding this protected information. This attestation applies to request for reproductive health care information related to one of the following purposes:
    - Health oversight activities
    - Judicial and administrative proceedings
    - Law enforcement purposes
    - Disclosures to coroners and medical examiners

Collection, Use and/or Disclosure where Authorization is Required

While there are instances where authorization is not required, as listed above, the following are some examples where authorization is required:

- Activities *other than* treatment, payment or health plan operations which involve the collection, use and/or disclosure of protected health information requires authorization. Please contact the Privacy Office and/or PHIVE Committee for guidance and approval.
  NOTE: Review Authorization and Consent Policy for specific requirements.
- Collection and use of biometric identifiers, such as voiceprint, requires:
    - Informing the individual or their legally authorized representative in writing before collecting and storing the biometric identifiers, including the purpose and length the identifier(s) are being collected and stored.
    - Receiving written consent to capture the biometric identifier, and
    - Destruction of the biometric identifier within a reasonable time, but not later than the first anniversary of the date the purpose for collecting the identifier expires.
- Sensitive Health Information – see definition. The disclosure of sensitive health information is strictly prohibited to *any party other than the subject of the information except under the following conditions:*
    - A member or patient's sensitive health information can be shared with the provider who originated the treatment and/or claims activity.
    - Information pertaining to mental or behavioral health may be disclosed to law enforcement in the event of a threat. See Duty to Warn Policy.
    - The member/patient is given an opportunity to provide informed, written consent permitting Humana to release the information to a third party.
    - Information relating to reproductive healthcare can be shared with a signed attestation that it is not for a prohibited purpose.

  NOTE: State laws may vary, and exceptions may apply. Public Health Reporting may be required. Contact the Privacy Office for understanding of disclosure of sensitive health information.
- Research: Humana Health Plan and Humana owned providers may not use and/or disclose protected health information for research without a written authorization from the individual. The only exception to this requirement is obtaining the appropriate written approval from an approved privacy board, or Institutional Review Board (IRB) to waive the authorization requirement. *Contact the PHIVE Committee and Humana's Law Department for guidance and approval on all research activities involving the use and/or disclosure of protected health information.*
- Marketing: Humana Health Plan and Humana owned providers will obtain a written authorization from the individual to whom the protected health information pertains prior to

any use and/or disclosure for any marketing activities with certain exceptions. Marketing activities that do not require authorization include:

- Face to face encounters with the individual (Ex: a pediatrician provides a free sample of formula and other baby products to new mothers after an office visit)
- Communications that include promotional gifts, products, or services of nominal value.

If marketing communication involves any direct or indirect remuneration to Humana from a third party, the authorization must state that such remuneration is involved.
The following activities are not considered marketing under the Privacy Rule:

- A communication is not considered marketing if it is to describe a health related product or service that is provided by or included in a Humana plan of benefits. This includes communications about providers participating in the network, replacement or enhancements to the health plan and health-related products or services available only to a health plan enrollee that add value to but are not part of benefits.
- Communications for treatment of the individual.
- Communications for case management or care coordination or treatment plan for the individual or to direct or recommend alternative treatments, therapies, health care providers or care settings to an individual.

Examples of marketing where authorization is required:

- A communication from a provider informing patients about a cardiac facility that is not part of the provider practice and can provide a baseline EKG for $39 when the communication is not for the purpose of providing treatment advice.
- A communication from a health insurer to their members promoting a home and casualty insurance product offered by the same company when the communication is not a health-related product or service or included in the member's plan of benefits.
- A health plan sharing a list of members to a Pharmacy (affiliated or nonaffiliated) which intends to send the plan member's brochures on the benefits of purchasing and using blood glucose monitors.

- Psychotherapy notes: Humana Health Plan and Humana owned providers will obtain a written authorization from the individual to use and/or disclose psychotherapy notes for activities outside of treatment, payment, or health plan operations.
- Fund-raising: Humana Health Plan and Humana owned providers do not engage in, sponsor, or sanction fund-raising activities that involve protected health information from Humana members/patients. All requests for fundraising projects involving protected health information must be directed to the Privacy Office for guidance and direction.

Prohibited Uses and Disclosures

- Paying Out of Pocket - An individual has the right to restrict disclosure of information to the health plan relating to services or treatments for which they paid out of pocket in full with the provider.
- Underwriting
  - Family History- Humana associates and business associates involved in underwriting activities/functions should not request or receive claims related information or ask questions regarding family history.
  - Use of Information collected for underwriting. If Humana receives protected health information for underwriting, premium rating, reinsurance activities or other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits and is not selected as the plan by the applicant, *Humana may not use and/or disclose such information for any other purpose except as required by law.*
  - Genetic Information use of genetic information, such as genetic tests or services, for underwriting purposes is prohibited.

- Reproductive Health Care
  - Releasing medical information that would identify an individual seeking or obtaining an abortion in response to a subpoena or a request to law enforcement if that subpoena, request, or the purpose of law enforcement for the medical information is based on, or for the purpose of enforcement of, either another state's laws or a foreign penal civil action, that interfere with a person's rights to choose or obtain an abortion is prohibited.
  - Releasing medical information to identify any person, for or to conduct a criminal, civil, or administrative investigation into, or impose such liability on any person for the act of seeking, obtaining, providing, or facilitating reproductive health care, where such health care is lawful under the circumstances in which it is provided is prohibited.

Disclosures by Whistleblowers

Humana associates, staff, or their business associates may disclose protected health information if they believe in good faith that Humana has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services or conditions provided by Humana potentially endangers one or more patients, workers or the public as long as the disclosure is directly to:

- A health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of Humana or to an appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by Humana; or
- An attorney retained by or on behalf of the Humana associate or business associate for the purpose of determining the legal options of the associate or business associate regarding the conduct.

Guidelines for Uses & Disclosures of Protected Health Information

Introduction

There are guidelines for safeguarding member and patient information that should be followed when conducting activities involving the use and/or disclosure of protected health information.

Authentication

Humana requires verification of the *identity* of a person whose protected health information is being requested prior to disclosing the information. Humana also verifies the *authority* of any person to have access to protected health information. Both identity and authority are required elements of the authentication process.

For example, the process of asking a series of questions is designed to validate the identity of the member or patient whose information is being requested while a Consent Form on file is designed to validate the authority or right of an individual to obtain protected health information.

Authentication is required for inbound and outbound communications, including telephone, e-mail, US postal service mail, and fax before disclosure of any protected health information. For telephone calls, voice recognition can be a form of authentication in instances where frequent contact with the same member/client/patient is common and as a result, the associate is familiar with and can recognize the member/client/patient.

Humana is permitted to leave messages with a family member or other person who answers the phone when the individual is not available. In addition, messages may be left for individuals on their answering machines. However, to reasonably safeguard the individual's privacy, Humana should take care to limit the amount of information disclosed on the message to the caller's name, company name, date and time, as applicable. In some situations, it may be appropriate to leave the caller's position or department name only if it does not reveal information specific to the individual's protected health information. For example, releasing Humana Beginnings as a department name may reveal the individual's health condition. In these situations, it would be more appropriate to state you are a registered nurse at Humana.

An authentication process is required for other telephone applications, such as Interactive Voice Response (IVR) and Voice Activated Technology (VAT) systems. Business is considered line 1 and is responsible for being TCPA compliant with outbound scripts, whether calls, text, or fax programs.

The Privacy - Guide for Disclosure of Information and Policy – Provider Privacy Guide for Disclosure of Information provides authenticating elements required prior to release of protected health information. These guides cover disclosures for all communication methods, including telephone, U.S. postal mail, email and fax. The guides can be found under the Privacy Office section of Policy Source.

Consent for Release of Protected Information Guidelines

Humana must obtain consent from members/patients when unauthorized representative's request protected information. The Corporate Consent Procedure provides information regarding the acceptable methods for submitting consent.

The purpose of this document is to provide guidelines for obtaining consent from members/patients before disclosing their protected information to other requestors.

Minimum Necessary

Minimum necessary is defined as limiting the use, disclosure, or request of protected health information to the least amount required to accomplish the intended purpose.

The minimum necessary requirement also includes limiting access to protected health information to those associates who have a "need to know" work function associated with their specific role at Humana.

Humana's minimum necessary requirement also includes oral communication and prohibits discussion beyond the least amount necessary to accomplish the intended purpose. Engaging in casual conversation regarding protected health information at any time either in an internal or external setting is prohibited.

Humana makes reasonable efforts to limit the use and disclosure of protected health information to the least amount required to accomplish the task, and applies the minimum necessary standards when requesting, using, or disclosing protected health information.

The minimum necessary requirement does NOT apply to:

- Uses or disclosures made to the individual who is the subject of the protected health information
- Uses or disclosures made pursuant to an individual's authorization
- Uses or disclosures required for compliance with HIPAA Administrative Simplification Rules
- Disclosures to a health care provider for treatment purposes
- Disclosures made to the Secretary of Health and Human Services when disclosure is required for enforcement purposes of the HIPAA Privacy regulations; or
- Uses or disclosures required by law.

Humana may presume that a request for information from public officials or covered entities (such as providers or hospitals) is for minimum necessary information.

De-Identification

De-identification is the process of removing key identifiers (name, address, SSN, etc.) from an individual's protected health information so that the remaining information no longer identifies the individual, and the information cannot be re-identified to the individual. De-identified data require no individual privacy protection and is not covered by the Privacy regulations.

Examples of when de-identification may be required would be reporting member/patient information to a fully insured group. This process is used to protect against improper disclosure. In certain circumstances, de-identification may also require removal of last two digits of zip code in sparsely populated geographic locations.

If a specific disclosure requires de-identification, contact the Privacy Office for assistance.

Re-Identification

Re-identification is the process of using a key (a unique code or mechanism) created during the de-identification process to re-identify previously de-identified information. If de-identified information requires re-identification, the Privacy Office must be contacted for assistance.

Limited Data Set

A limited data set is protected health information that excludes specific direct identifiers but may contain more identifiers than de-identified data. A limited data set may be created, used, or disclosed

only for the purposes of research, health plan operations and public health purposes if a valid Data Use Agreement is obtained from the recipient. This process can be used as an alternative to de-identifying data.

Contact the Privacy Office for guidance on the creation of limited data sets.

Routine Uses and/or Disclosures

Routine disclosures of protected health information that ordinarily happen in routine payment and health plan operations or on a recurring basis. Formal approval must be provided prior to any initial routine disclosure. All documentation must be submitted to the Privacy Office for review and approval.

- For treatment
- To obtain payment for treatment
- For healthcare operations
- To Business Associates for treatment, payment, and heath care operations
- Individuals involved in your care or payment for your care
- Appointment reminders
- Treatment alternatives
- Health related benefits and services
- Worker's compensation.

Non-Routine Uses and/or Disclosures

A non-routine disclosure is a request for disclosure of protected health information that does not ordinarily happen in routine operations or on a recurring basis. The request could be for a special situation or an exception to the normal process. Some- examples include, but are not limited to:

- Court orders
- External audits
- Marketing
- Medical Research
- Requests from attorneys or law firms
- Subpoenas.

If the request is for a non-routine disclosure of protected health information for legal proceedings (judicial or administrative), the request must be routed to the appropriate Critical Inquiry Department or risk manager. Examples of these requests include court orders, subpoenas, or other requests from attorneys or law firms.

All other requests for non-routine disclosure of protected health information must be forwarded to the Privacy Office for approval. Examples could include, but are not limited to, marketing and medical research activities.

PHIVE Committee

Humana's Protected Health Information and Vendor Ethics (PHIVE) Committee is a multidisciplinary committee whose focus is on the protection of individually identifiable health information of Humana members and patients and on the application of professional standards related to industry/vendor supported educational activities and joint ventures. The PHIVE Committee has the authority to set and apply protected health information (PHI) and vendor ethics (VE) guidance to internal and external business activities.

The primary business need for the PHIVE Committee is to review and approve or deny the following:

- Any program, outside normal health plan operations, that includes the use or disclosure of individually identifiable health information including health information thought to be de-identified. This includes all clinical research which is either externally or internally sponsored.
- All joint ventures with vendors, such as pharmaceutical companies, that involve the receipt of remuneration or service to Humana from the vendor that is not payment for services or goods received.

Any activities that fall within this scope must be reviewed and approved by the PHIVE Committee which meets on the third Friday of each month. The deadline for proposals to be reviewed is the first Friday of each month.

If you have any questions about the PHIVE Committee or would like to know how to submit a proposal for review by the PHIVE Committee, send an e-mail to PHIVE@humana.com.

Business Associate and Third-Party Requirements

Business Associate

A business associate is a person or entity that provides services on behalf of Humana that involve the creation, transfer, storage, use, and/or access to protected health information.

- Business Associates and their subcontractors are directly subject to criminal and civil sanctions for violation of HIPAA's Privacy and Security Rules to the same extent as Covered Entities.
- Business Associate becomes liable when they are involved in the creation, receipt, maintenance, storage, or transmission of Protected Health Information on behalf of a Covered Entity regardless of whether or not a Business Associate Agreement has been completed.

Examples of Business Associates functions conducted on behalf of Humana include but are not limited to:

- Claim processing
- Billing functions
- Disease management
- External Review Organizations
- Data file/storage
- Delegates
- Outsourcing services
- Transcriptionist
- Collection Agencies
- Data Analysis
- Electronic Medical Records provider
- Healthcare equipment company
- Evaluation of health care professionals.

Examples of business associates who provide service to Humana include but are not limited to:

- Health Information Organizations (including health information exchanges)
- e-prescribing gateways
- Actuarial
- Consulting
- Financial
- Legal
- Quality Assurance.

Examples of entities that are not considered business associates are:

- Government Agencies.
- A health care provider with respect to disclosures by a covered entity to the health care provider concerning the treatment of the individual.
- A plan sponsor such as a Fully Insured Group.

Humana requires a written agreement, called a Business Associate Agreement, with any person or entity acting as a business associate. This agreement contains specific language and requirements providing safeguards for protected health information from misuse and inappropriate disclosure.

Before disclosing protected health information to an external entity, you should determine if Humana has a signed Business Associate Agreement with that entity and that the information being disclosed is permissible under the terms of the agreement.

You can determine if a Business Associate Agreement exists by viewing the Business Associate Listing link on the Privacy Web Site, or by contacting the Privacy Office.

If the external entity is not found on the listing, do not disclose any protected health information, and contact the Privacy Office for guidance.

If it is your responsibility to contract with an external entity where Humana is disclosing protected health information. It is also your responsibility to execute a Business Associate Agreement with that external entity. Refer to the document Business Associate Agreements or the Privacy Office for guidance.

Humana as a Business Associate

There are some situations where Humana acts as a business associate by performing functions involving the use and disclosure of protected health information on behalf of another covered entity. In those situations, the covered entity requires Humana to enter into a Business Associate Agreement.

In general, situations where Humana is considered the business associate occur when we are functioning as a third-party payer for self-funded groups, Flexible Spending Account (FSA), Personal Care Account (PCA), and Health Savings Account (HSA) products.

Before disclosing protected health information on a group's behalf for all self-funded, FSA, PCA, and HSA products, you should determine if Humana has received the appropriate documentation from the group and that the individual requesting the information is authorized to receive such information. This information is contained within the Group Authorized Recipient Privacy (GARP) database. Refer to the document GARP Database Procedure for additional information on how to access and use this database.

Before using protected health information on a group's behalf for all self-funded, FSA, PCA, and HSA products, you must review the Business Associate Agreement. This agreement outlines Humana's obligations as to how we may use and disclose their member protected health information as necessary to preform our functions as a third party. Any uses outside of necessary functions, such as marketing, etc. must be reviewed and approved by the Privacy Office. Contact the Privacy Office for guidance and review the Business Associate Agreement.

It is your responsibility to contract with an external entity where Humana is acting as a business associate involving the use and disclosure of protected health information on behalf of another covered entity. It is also your responsibility to ensure a Business Associate Agreement and/or Plan Sponsor Certification has been executed and completed with that covered entity following your area procedures. Contact the Privacy Office for guidance.

Covered Entity with Multiple Covered Functions

Humana, the company, has many different entities that provide services to many different customers. The different Humana entities include:

- Insurance Organization (medical, dental and vision)
- Physician Organization (CenterWell Primary Care, Conviva, Elite, CenterWell Home Health and Onehome)
- Pharmacy Services (For example CenterWell Pharmacy - Mail Order Pharmacy, CenterWell Pharmacy - Specialty Pharmacy, CenterWell Retail Pharmacy and Enclara)
- Wellness and Prevention Services (For example Humana Behavioral Health, Go365, etc.)

- Chronic Care Services (For example Humana at Home, American Eldercare)
- Informatics Services (For example Transcends Insights)

The HIPAA Privacy Rule considers each of these entities as unique and separate with respect to the collection, the use, and the disclosure of individually identifiable information. Restrictions, limitations, and requirements exist on the exchange/disclosure/sharing of individually identifiable information between these Humana entities.

Reporting a Suspected Privacy Incident or Breach by a Business Associate or External Entity

All suspected incidents, breaches or violations by a business associate or external entity must be reported to the Privacy Office immediately upon discovery. The suspected incident breach or violation is investigated, and appropriate action taken by the Privacy Office.

If the corrective actions taken with our business associate or external entity are unsuccessful, Humana may terminate the Agreement or report the problem to the U.S. Department of Health and Human Services.

Safeguards

Technical and Physical Safeguards

Humana maintains reasonable technical and physical safeguards to protect the privacy of protected information from any intentional or unintentional use or disclosure, or violation of the privacy policy and standards.

Protected information may only be accessed, created, stored, sent (uploaded), received (downloaded), or transported in accordance with Humana's *Information Protection Acceptable Use Policy* and the *Physical and Environmental Security*.

See also, *Clean Desk, Clean Screen Standard*.

System Access and Use

When protected information is accessed, created, stored, sent (uploaded), received (downloaded) or transported using Humana Information Technology Systems, please refer to the *EIP Secured Data Handling Standard*, the *Information Protection Acceptable Use Policy* and the *Physical and Environmental Security* for guidance.

Electronic Disclosure

Uses and disclosures of protected information via any electronic means, including fax and e-mail, are made using a secure and appropriate manner. For additional details, see Humana's *Information Protection Acceptable Use Policy* and Communication Security for guidance.

Website Internet Privacy Statement

External facing websites published and maintained by Humana and/or any Humana subsidiaries must include standard format and content as described in Humana's Corporate Website Internet Privacy Statement Standard.

Records Retention and Disposal

Humana keeps documents containing protected information as required by state and/or federal laws, rules, standards, and regulations, and in accordance with Humana's records retention program. With the permission of the Law Department, protected information should be destroyed in a manner that precludes identification of the individual and subject matter. See Humana's program description in the document *Records Retention Policy*.

Off-site paper records are stored according to the vendor's storage process as approved by Humana. Access the records retention schedule, and the Policies and Procedures Manual on the Humana Records Management Portal.

Storage and Transport of Protected Information

In general, protected information should not be removed from Humana facilities for use offsite. This includes removing papers, emailing, or using electronic media of any kind to transfer or transport protected information for offsite use, or use on a non-Humana computer, such as working on a home personal computer.

While it is not general practice, Humana is aware of unique job roles that may require the removal of or shipment of protected information to perform treatment, payment, and health care operations. In those situations, the department must develop and implement procedures:

- For verifying that the protected information is secure while offsite, and
- That documents are returned to the site as soon as is reasonably possible. These procedures should verify that:
- Removal of the protected information is for an appropriate reason and that other options involving less risk are not available
- Documents removed are inventoried and trackable. If shipped using a courier such as UPS or FedEX, a tracking number must be obtained, and all information must be maintained by the sender related to content in the event material sent must be reproduced
- Protected information (specific content) is logged and approved by the appropriate departmental leader prior to removal and return is verified
- The location and possessor of the protected information is known at all times
- Associates take reasonable precautions to protect the physical integrity, security and confidentiality of the protected information
- The protected information is returned to the facility within a set period
- Any damage to, loss of, or unauthorized access to the protected information is promptly reported to the department leader and the process for *Reporting a Suspected Privacy or Security Policy Violation* is followed.

See Humana's *Information Protection Acceptable Use Policy* and the *Physical and Environmental Security*.

Termination of Employment

All conditions and restrictions in force by the execution of Humana's Confidentiality Agreement and the Conflict of Interest Information Disclosure and Agreement continue to apply when an associate's employment with Humana is terminated.

Associate Information

Reporting a Suspected Privacy Incident, Breach or Violation

Any Humana associate or colleague having knowledge of a violation or potential violation of the privacy policies and standards should report the incident. Suspected violations of privacy and/or security policies should be reported promptly using the internal communication process. Choose the step you feel most comfortable following:

- Report the issue to your supervisor or manager
- Report the issue to your supervisor's immediate manager or the next level of management
- Report the issue to HR4U (1-888-431-4748) (where applicable)
- Report the issue to the Humana Resources Department consultant assigned to your area, or to the Associate Relations Department
- Report the issue to the Humana Ethics Office via e-mail:
- Internet e-mail at: ethicsoffice@humana.com.
- Call the Ethics Help Line at 1-877-584-3539 (1-877-5 THE KEY).

**Note: If you are an associate in management or a supervisory role, upon receipt of the report of a suspected violation, contact the Ethics Office or the Ethics Help Line. See also, *Ethics Every Day* and *Reporting a Suspected Privacy or Security Breach*.

Associates have the option to remain anonymous when reporting a privacy issue.

Associates should report any suspected privacy incident, breach or violation by a business associate immediately. The Privacy Office investigates and takes appropriate actions. If the corrective actions taken with our business associates are unsuccessful, Humana may terminate the agreement or report the problem to the U.S. Department of Health and Human Services.

If you have questions regarding what constitutes a privacy incident or breach, contact the Privacy Office for guidance via email at privacyoffice@humana.com.

Humana will not intimidate, threaten, coerce, or take retaliation against any associate, individual, business associate, or other person for reporting an alleged privacy incident or breach, or participating in an investigation, compliance review, proceeding, or hearing.

Penalties for Non-Compliance

Humana associates and colleagues who violate or fail to comply with Humana's *Privacy Policies and Standards* are subject to disciplinary actions, up to and including termination of employment, and may also be subject to civil penalties.

Definitions

- Policy - Privacy Definitions

Index

Owner:	Mark W. Ianke	**Executive Team Member:**	Joe Ventura
Accountable VP / Director:	Dana Cox		

Disclaimer:

Humana follows all federal and state laws and regulations. Where more than one state is impacted by an issue, to allow for consistency, Humana will follow the most stringent requirement.

This document is intended as a guideline. Situations may arise in which professional judgment may necessitate actions that differ from the guideline. Circumstances that justify the variation from the guidelines should be noted and submitted to the appropriate business area for review and documentation. This (policy/procedure) is subject to change or termination by Humana at any time. Humana has full and final discretionary authority for its interpretation and application. This (policy/procedure) supersedes all other policies, requirements, procedures, or information conflicting with it. If viewing a printed version of this document, please refer to the electronic copy maintained in Policy Source to ensure no modifications have been made.

Non-Compliance:

Failure to comply with any part of Humana's policies, procedures, and guidelines may result in disciplinary actions up to and including termination of employment, services, or relationship with Humana. In addition, state and/or federal agencies may take action in accordance with applicable laws, rules and regulations.

Any unlawful act involving Humana systems or information may result in Humana turning over all evidence of unlawful activity to appropriate authorities. Information on handling sanctions related to noncompliance with this policy may be found in the Expectations for Performance, and Critical Offenses policies, both of which may be found in the Associate Support Center via Humana's secure intranet on Hi! (Workday & Apps/Associate Support Center).