DENTAL PROVIDER MANUAL
(Provider Handbook)

Passport by Molina Healthcare, Inc.
(Passport)

Medicaid
2026

Capitalized words or phrases used in this Provider Manual shall have the meaning set forth in the Provider Agreement with Passport by Molina Healthcare. “Passport” has the same meaning as “Health Plan” in your Agreement. The Provider Manual is customarily updated annually but may be updated more frequently as needed. Providers can access the most current Provider Manual at PossportHeolthPlon.com.

Last Updated 12/2025

MHKY 2814 APP 01/05/2025

PASSPORT
BY MOLINA HEALTHCARE

Table of Contents

1. Contact Information

Passport by Molina Healthcare
2028 W. Broadway
Louisville, KY 40203

Provider Services

The SKYGEN Provider Contact Center handles telephone inquiries from Providers regarding Claims, appeals, authorizations, eligibility, and general concerns. SKYGEN Contact Center representatives are available 8 am to 6 pm, Eastern Time excluding state and federal holidays.

Eligibility verifications can be conducted at your convenience via the Eligibility and Benefits module on the SKYGEN portal.

Phone: (855) 994-2453
SKYGEN portal: SKYGEN
Hearing Impaired (TTY/TDD): 711

Provider Relations

The Provider Relations department manages Provider issue resolution, Provider education and training. The department has Provider Relations representatives who serve all of Passport's Provider network and are available via email, phone and fax at the following:

MDVSProviderServices@MolinaHealthcare.com
Phone: (844) 862-4564
Hearing Impaired: 711
Fax: (855) 297-3304

Member Services

The Passport Member Contact Center handles all telephone inquiries regarding benefits, eligibility/identification, pharmacy inquiries, selecting or changing primary care dentists (PCD) and Member complaints. Passport Member Contact Center representatives are available 7:00 a.m. to 7:00 p.m. Monday through Friday, excluding state and federal holidays.
Phone: (800) 578-0603
Hearing Impaired (TTY/TDD): 711

Claims

Passport strongly encourages participating Providers to submit Claims electronically via a clearinghouse or the SKYGEN Hub whenever possible.

- EDI Payer ID Number: SKYGN without the "E"

To verify the status of your Claims please use the SKYGEN portal. Claims questions can be submitted through the Secure Messaging feature via the Claim Status module on the SKYGEN portal, or by contacting the SKYGEN Contact Center.

To verify the status of your Claims, please use the SKYGEN portal. Claims questions can be submitted through the Secure Messaging feature via the Claim Status module on the SKYGEN portal or by contacting the SKYGEN Contact Center. For additional information please refer to the **Claims and Compensation** section of this Provider Manual.
Phone: (855) 994-2453.

Claims Recovery

The Claims Recovery department manages recovery for overpayment and incorrect payment of Claims.

Provider Overpayment Disputes/Refund checks	Molina Healthcare of Kentucky, Inc. Molina KY Refunds PO Box 641 Milwaukee, WI 53201
Phone:	(855) 994-2453
SKYGEN Dental HUB	https://app.dentalHUB.com/app/login

Compliance and Fraud AlertLine

Suspected cases of fraud, waste or abuse must be reported to Passport. You may do so by contacting the Passport AlertLine or by submitting an electronic complaint using the website listed below. For additional information on fraud, waste and abuse please refer to the **Compliance** section of this Provider Manual.

Confidential Compliance Officer
Passport by Molina Healthcare
2028 W. Broadway
Louisville, KY 40203
Phone: (866) 606-3889
Online: MolinaHealthcare.Alertline.com

Credentialing

The Credentialing department verifies all information on the Provider Application prior to contracting and re-verifies this information every three (3) years or sooner depending on Passport's credentialing criteria. The information is then presented to the Professional Review Committee to evaluate a Provider's qualifications to participate in the Passport network. For additional information about Passport's credentialing program please refer to the **Network Participation** section of this Provider Manual.

24-hour Nurse Advice Line

This telephone-based nurse advice line is available to all Passport Members. Members may call anytime they are experiencing symptoms or need Healthcare information. Registered nurses are available 24 hours a day, 7 days a week.

- Phone: (800) 606-9880
- Hearing Impaired (TTY/TDD): 711

Healthcare Services

The Healthcare Services (HCS) department conducts concurrent review on inpatient cases and processes prior authorizations/service requests. The HCS department also performs care management for Members who will benefit from care management services. Participating Providers are required to interact with Passport's HCS department electronically whenever possible. Prior authorizations/service requests and status checks can be easily managed electronically. For additional information please refer to the **Healthcare Services** section of this Provider Manual.

Managing prior authorizations/service requests electronically provides many benefits to Providers, such as:

- Easy to access 24/7 online submission and status checks
- Ensures Health Insurance Portability and Accountability Act (HIPAA) compliance
- Ability to receive real-time authorization status
- Ability to upload medical records
- Increased efficiencies through reduced telephonic interactions
- Reduces costs associated with fax and telephonic interactions

Pharmacy

The prescription drug benefit is administered through MedImpact. A list of in-network pharmacies is available on the passporthealthplan.com website or by contacting Passport at (800) 210-7628. For additional information, please refer to the **Pharmacy** section of this Provider Manual.

Quality

Passport maintains a Quality department to work with Members and Providers in administering the Passport Quality Improvement (QI) Program. For additional information please refer to the **Quality** section of this Provider Manual.

Phone: (800) 578-0775

Passport by Molina Healthcare Service Area

2. Provider Responsibilities

Non-discrimination in Healthcare Service Delivery

Providers must comply with the nondiscrimination in healthcare service delivery requirements as outlined in the **Culturally Linguistically Appropriate Services** section of this Provider Manual.

Additionally, Passport requires Providers to deliver services to Passport Members without regard to the source of payment. Specifically, Providers may not refuse to serve Passport Members because they receive assistance with cost-sharing from a government-funded program. Providers serving Medicaid Members are required to maintain the same hours of operation as those offered to commercial benefit Members.

Section 1557 Investigations

All Passport Providers shall disclose all investigations conducted pursuant to Section 1557 of the Patient Protection and Affordable Care Act to Passport's Civil Rights Coordinator.

Passport by Molina Healthcare Civil Rights
Coordinator
2028 W. Broadway
Louisville, KY 40203
Toll Free: (866) 606-3889
TTY/TDD: 711
Online: https://MolinaHealthcare.AlertLine.com

Email: civil.rights@passporthealth.com

Should you or a Passport Member need more information, you can refer to the Health and Human Services website: HHS WEBSITE

Facilities, Equipment, Personnel, and Administrative Services

The Provider's facilities, equipment, personnel, and administrative services must be at a level and quality necessary to perform duties and responsibilities to meet all applicable legal requirements including the accessibility requirements of the Americans with Disabilities Act (ADA).

Provider Data Accuracy and Validation

It is important for Providers to ensure Passport has accurate practice and business information. Accurate information allows us to better support and serve our Members and Provider Network.

Maintaining an accurate and current Provider Directory is a state and federal regulatory requirement, as well as an NCQA-required element. Invalid information can negatively impact Member access to care, Member/PCD assignments and referrals. Additionally, current information is critical for timely and accurate Claims processing.

Providers must validate their Provider information on file with Passport at least once every 90 days for correctness and completeness.

Additionally, in accordance with the terms specified in the Provider Agreement with Passport, Providers must notify Passport of any changes, as soon as possible, but at a minimum 30 calendar days in advance of any changes in any Provider information on file with Passport. Changes include, but are not limited to:

- Change in office location(s)/address, office hours, phone, fax, or email
- Addition or closure of office location(s)
- Addition of a Provider (within an existing clinic/practice)
- Change in Provider or practice name, Tax ID, and/or National Provider Identifier (NPI)
- Opening or closing your practice to new patients (PCDs only)
- Change in specialty
- Any other information that may impact Member access to care

For Provider terminations (within an existing clinic/practice), Providers must notify Passport in writing in accordance with the terms specified in your Provider Agreement with Passport.

Please visit our Provider Online Directory at https://www.passporthealthplan.com/ to validate your information. Providers can make updates through the Council for Affordable Quality Healthcare's CAQH portal or you may submit a full roster that includes the required information above for each Healthcare Provider and/or Healthcare facility in your practice. Providers unable

to make updates through the CAQH portal or roster process should contact their Passport Provider Relations representative for assistance.

Note: Some changes may impact credentialing. Providers are required to notify Passport of changes to credentialing information in accordance with the requirements outlined in the **Network Participation** section of this Provider Manual.

Passport is required to audit and validate our Provider network data and Provider directories on a routine basis. As part of our validation efforts, we may reach out to our network of Providers through various methods, such as letters, phone campaigns, face-to-face contact, fax, and fax-back verification, etc. Passport also may use a vendor to conduct routine outreach to validate data that impacts the Provider directory or otherwise impacts its membership or ability to coordinate Member care. Providers are required to supply timely responses to such communications.

All Passport Providers participating in a Medicaid network must be enrolled in the state Medicaid program to be eligible for reimbursement. If a Provider has not had a Medicaid number assigned, the Provider must apply for enrollment with the https://medicaidsystems.ky.gov/Partnerportal/home.aspx and meet the Medicaid Provider enrollment requirements set forth in the Department for Medicaid Services (DMS) and meet the Medicaid Provider enrollment requirements set forth in the Kentucky Administrative Regulations and in the Medicaid policy and procedures manual for fee-for-service Providers of the appropriate provider type.

National Plan and Provider Enumeration System (NPPES) Data Verification

In addition to the above verification requirements, the Centers for Medicare & Medicaid Services (CMS) recommends that Providers routinely verify and attest to the accuracy of their NPPES data.

NPPES allows Providers to attest to the accuracy of their data. If the data is correct, the Provider can attest and NPPES will reflect the attestation date. If the information is not correct, the Provider is able to request a change to the record and attest to the changed data, resulting in an updated certification date.

Passport supports the CMS recommendations around NPPES data verification and encourages our Provider network to verify Provider data via nppes.cms.hhs.gov. Passport may validate the NPI submitted in a Claim transaction is a valid NPI and is recognized as part of the NPPES data. Additional information regarding the use of NPPES is available in the Frequently Asked Questions (FAQ) document published at cms.gov/Medicare/Health-Plans/ManagedCareMarketing/index.

Passport Electronic Solutions Requirements

Passport requires Providers to utilize electronic solutions and tools whenever possible.

Passport requires all contracted Providers to participate in and comply with Passport's electronic solution requirements, which include, but are not limited to, electronic submission of prior authorization requests, prior authorization status inquiries, health plan access to electronic medical records (EMR), electronic Claim submission, electronic fund transfers (EFT), electronic remittance advice (ERA), electronic Claim Appeal and registration for and use of the SKYGEN portal.

Electronic Claims include Claims submitted via a clearinghouse using the EDI process and Claims submitted through the SKYGEN portal.

Any Provider entering the network as a contracted Provider will be encouraged to comply with Passport's electronic solution policy by enrolling for EFT/ERA payments and registering for the SKYGEN portal within 30 days of entering the Passport network.

Passport is committed to complying with all HIPAA Transactions, Code Sets, and Identifiers (TCI) standards. Providers must comply with all HIPAA requirements when using electronic solutions with Passport. Providers must obtain an NPI and use their NPI in HIPAA transactions, including Claims submitted to Passport. Providers may obtain additional information by visiting Passport's HIPAA Resource Center located on our website at MolinaHealthcare.com.

Electronic Solutions/Tools Available to Providers

Electronic solutions/tools available to Passport Providers include:

- Electronic Claim submission options
- Electronic payment: EFT with ERA
- SKYGEN portal

Electronic Claim Submission Requirement

Passport strongly encourages participating Providers to submit Claims electronically whenever possible. Electronic Claim submission provides significant benefits to the Provider such as:

- Promoting HIPAA compliance
- Helping to reduce operational costs associated with paper Claims (printing, postage, etc.)
- Increasing accuracy of data and efficient information delivery
- Reducing Claim processing delays as errors can be corrected and resubmitted electronically
- Eliminating mailing time and enabling Claims to reach Passport faster

Passport offers the following electronic Claim submission options:

- Submit Claims directly to Passport via the SKYGEN portal
- Submit Claims to Passport through your EDI clearinghouse using Payer ID SKYGN Please refer to our website at MolinaHealthcare.com for additional information.

While both options are embraced by Passport, submitting Claims via the SKYGEN portal (available to all Providers at no cost) offers several additional Claim processing benefits beyond the possible cost savings achieved from the reduction of high-cost paper Claims.

SKYGEN portal Claim submission includes the ability to:

- Add attachments to Claims
- Submit corrected Claims
- Easily and quickly void Claims
- Check Claim status
- Receive timely notification of a change in status for a particular Claim
- Ability to save incomplete/un-submitted Claims
- Create/manage Claim templates

For additional information on EDI Claim submission and Paper Claim submission please refer to the **Claims and Compensation** section of this Provider Manual.

Electronic Payment Requirement

Participating Providers are encouraged to enroll in EFT and ERA. Providers enrolled in EFT payments will automatically receive ERAs on the SKYGEN Dental Hub as well. EFT/ERA services give Providers the ability to reduce paperwork, utilize searchable ERAs and receive payment and ERA access faster than the paper check and remittance advice (RA) processes. There is no cost to the Provider for EFT enrollment and Providers are not required to be in-network to enroll. Passport uses a vendor to facilitate the HIPAA-compliant EFT payment and ERA delivery processes.

As a reminder, Passport's Payer ID is SKYGN without the "E."

Once your account is activated, you will begin receiving all payments through EFT and you will no longer receive a paper EOP (i.e., remittance) through the mail. You will receive 835s (by your selection of routing or via manual download) and can view, print, download and save historical and new ERAs with a two (2)-year lookback.

Additional instructions on how to register are available under the EDI/ERA/EFT tab on Passport's website at MolinaHealthcare.com.

SKYGEN Dental Hub

Providers and third-party billers can use the no-cost SKYGEN portal to perform many functions online without the need to call or fax Passport. Registration can be performed online and once completed the easy-to-use tool offers the following features:

- Verify Member eligibility, covered services and view Healthcare Effectiveness Data and Information Set (HEDIS®) needed services (gaps)
- Claims:

- Submit Professional ADA Claims with attached files
- Correct/void Claims
- Add attachments to previously submitted Claims
- Check Claim status
- View ERA and EOP
- Create and manage Claim templates
- Create and submit a Claim appeal with attached files
- Prior authorizations/service requests
- Create and submit prior authorization/service requests
- Check status of prior authorization/service requests
- Download forms and documents

HEDIS® is a registered trademark of the National Committee for Quality Assurance (NCQA)

Balance Billing

The Provider is responsible for verifying eligibility and obtaining approval for those services that require prior authorization. Providers agree that under no circumstance shall a Member be liable to the Provider for any sums that are the legal obligation of Passport to the Provider. Balance billing a Passport Member for Covered Services is prohibited, except for the Member's applicable copayment, coinsurance, and deductible amounts. However, if a Member agrees in advance in writing to pay for a Non-Medicaid covered service, then Passport, Passport's Provider, or Passport's Subcontractor may bill the Member. The standard release form signed by the Member at the time of services does not relieve Passport, Providers and Subcontractors from the prohibition against billing a Medicaid Member in the absence of a knowing assumption of liability for a Non-Medicaid Covered Services. The form or other type of acknowledgement relevant to the Medicaid Member liability must specifically state the services or procedures that are not covered by Medicaid. Any Provider who knowingly and willfully bills a Member for a Medicaid Covered Service shall be guilty of a felony and upon conviction shall be fined, imprisoned, or both, as defined in Section 1128B(d)(1) 42 U.S.C. 1320a-7b of the Social Security Act. This provision shall remain in effect even if Passport becomes insolvent.

Member Rights and Responsibilities

Providers are required to comply with the Member Rights and Responsibilities as outlined in Passport's Member materials (such as Member Handbooks).

For additional information please refer to the **Member Rights and Responsibilities** section in this Provider Manual.

Member Information and Marketing

Any written informational or marketing materials directed to Passport Members must be developed and distributed in a manner compliant with all state and federal laws and regulations and approved by Passport prior to use.

Please contact their Passport Provider Relations representative for information and review of proposed materials.

Member Eligibility Verification

Possession of a Passport Member ID card does not guarantee Member eligibility or coverage. Providers should verify the eligibility of Passport Members prior to rendering services. Payment for services rendered is based on enrollment and benefit eligibility. The contractual agreement between Providers and Passport places the responsibility for eligibility verification on the Provider of services.

Providers who contract with Passport may verify a Member's eligibility by checking the following:

- SKYGEN

Passport Provider Contact Center automated Interactive Voice Response (IVR) system at (855) 994-2453.

For additional information please refer to the **Eligibility, Enrollment, Disenrollment and Grace Period** section of this Provider Manual.

Member Cost Share

Providers should verify the Passport Member's cost share status prior to requiring the Member to pay co-pay, co-insurance, deductible, or other cost share that may be applicable to the Member's specific benefit plan. Some plans have a total maximum cost share that frees the Member from any further out-of-pocket charges once reached (during that calendar year).

Healthcare Services (Utilization Management and Care Management)

Providers are required to participate in and comply with Passport's utilization management and care management programs, including all policies and procedures regarding Passport's facility admission, prior authorization, medical necessity review determination and Interdisciplinary Care Team (ICT) procedures. Providers will also cooperate with Passport in audits to identify, confirm, and/or assess utilization levels of covered services.

For additional information please refer to the **Healthcare Services** section of this Provider Manual

Treatment Alternatives and Communication with Members

Passport endorses open Provider-Member communication regarding appropriate treatment alternatives and any follow-up care. Passport promotes open discussion between Providers and Members regarding medically necessary or appropriate patient care, regardless of covered benefits limitations. Providers are free to communicate all treatment options to Members

regardless of benefit coverage limitations. Providers are also encouraged to promote and facilitate training in self-care and other measures Members may take to promote their own health.

Pharmacy Program

Providers are required to adhere to Passport's drug formularies and prescription policies. For additional information please refer to the **Pharmacy** section of this Provider Manual.

Participation in Quality Improvement (QI) Programs

Providers are expected to participate in Passport's QI Programs and collaborate with Passport in conducting peer review and audits of care rendered by Providers. Such participation includes, but is not limited to:

- Access to care standards
- Site and medical record-keeping practice reviews as applicable
- Delivery of patient care information

For additional information please refer to the **Quality** section of this Provider Manual.

Compliance

Providers must comply with all state and federal laws and regulations related to the care and management of Passport Members.

Confidentiality of Member Health Information and HIPAA Transactions

Password requires that Providers respect the privacy of Passport Members (including Passport Members who are not patients of the Provider) and comply with all applicable laws and regulations regarding the privacy of patient and Member protected health information.

For additional information please refer to the **Compliance** section of this Provider Manual.

Participation in Grievance and Appeals Programs

Providers are required to participate in Passport's grievance and appeals programs and cooperate with Passport in identifying, processing and promptly resolving all Member complaints, grievances, or inquiries. If a Member has a complaint regarding a Provider, the Provider will participate in the investigation of the grievance. If a Member submits an appeal, the Provider will participate by providing medical records or statements if needed. This includes the maintenance and retention of Member records for a period of not less than 10 years and retained further if the records are under review or audit until such time that the review or audit is complete.

For additional information please refer to the **Complaints, Grievance and Appeals Process** section of this Provider Manual.

Participation in Credentialing

Providers are required to participate in Passport's credentialing and re-credentialing process and will satisfy, throughout the term of their contract, all credentialing and re-credentialing criteria established by Passport and applicable accreditation, state, and federal requirements. This includes providing prompt responses to Passport's requests for information related to the credentialing or re-credentialing process.

For additional information on Passport's credentialing program please refer to the **Network Participation** section of this Provider Manual.

Delegation

Delegated entities must comply with the terms and conditions outlined in Passport's Delegated Services Addendum. For additional information on Passport's delegation requirements and delegation oversight please refer to the **Delegation** section of this Provider Manual.

Primary Care Provider Responsibilities

PCDs are responsible to:

- Serve as the ongoing source of primary and preventive care for Members
- Assist with coordination of care as appropriate for the Member's Healthcare needs
- Recommend referrals to specialists participating with Passport
- Triage appropriately
- Notify Passport of Members who may benefit from care management
- Participate in the development of care management treatment plans

3. Cultural Competency and Linguistic Services

Background

Passport works to ensure all Members receive culturally competent care across the service continuum to reduce health disparities and improve health outcomes. The Culturally and Linguistically Appropriate Services in Healthcare (CLAS) standards published by the U.S. Department of Health and Human Services (HHS), Office of Minority Health (OMH) guide the activities to deliver culturally competent services. Passport complies with Section 1557 of the ACA, prohibiting discrimination in health programs and activities receiving federal financial assistance on the basis of race, color and national origin, sex, age and disability per Title VI of the Civil Rights Act of 1964, Title IX of the Education Amendments of 1972, the Age Discrimination Act of 1975 and Section 504 of the Rehabilitation Act of 1975 (29 U.S.C. § 794). Passport complies with applicable portions of the Americans with Disabilities Act of 1990. Passport also complies with all implementing regulations for the foregoing. Compliance ensures

the provision of linguistic access and disability-related access to all Members, including those with Limited English Proficiency (LEP) and Members who are deaf, hard of hearing, non-verbal, have a speech impairment or have an intellectual disability. Policies and procedures address how individuals and systems within the organization will effectively provide services to people of all cultures, races, ethnic backgrounds, genders, gender identities, sexual orientations, ages, and religions, as well as those with disabilities in a manner that recognizes values, affirms, and respects the worth of the individuals and protects and preserves the dignity of each.

Additional information on cultural competency and linguistic services is available at MolinaHealthcare.com, from local Passport Provider relations representatives or by calling the Passport Provider Contact Center at (855) 994-2453.

Non-discrimination in Healthcare Service Delivery

Passport complies with Section 1557 of the ACA. As a Provider participating in Passport's Provider Network, you and your staff must also comply with the nondiscrimination provisions and guidance set forth by the Department of Health and Human Services, Office for Civil Rights (HHS-OCR), state law and federal program rules, including Section 1557 of the ACA.
You are required to do, at a minimum, the following:

1. You **MAY NOT** limit your practice because of a Member's medical (physical or mental) condition or the expectation for the need of frequent or high-cost care.
2. You **MUST** post in a conspicuous location in your office a Nondiscrimination Notice. A sample of the Nondiscrimination Notice that you will post can be found in the Member Handbook located at http://molinahealthcare.com/members/ky/en-US/mem/medicaid/overvw/handbook
3. You **MUST** post in a conspicuous location in your office a Tagline Document that explains how to access non-English language services. A sample of the Tagline Document that you will post can be found in the Tagline Document found in the Member Handbook located at http://molinahealthcare.com/members/ky/enUS/mem/medicaid/overvw/handbook
4. If a Passport Member is in need of language assistance services while at your office and you are a recipient of federal financial assistance, you **MUST** take reasonable steps to make your services accessible to persons with LEP. You can find resources on meeting your LEP obligations at hhs.gov/civil-rights/for-individuals/special-topics/limited-english-proficiency/index and hhs.gov/civil-rights/for-providers/clearance-medicare-providers/technical-assistance/limited-english-proficiency/index.
5. If a Passport Member complains of discrimination, you **MUST** provide them with the following information so that they may file a complaint with Passport's Civil Rights Coordinator or the HHS-OCR:

Civil Rights Coordinator Molina Healthcare, Inc. 200 Oceangate, Suite 100 Long Beach, CA 90802 Phone (866) 606-3889 (TTY/TDD, 711) civil.rights@passporthealth.com	Office of Civil Rights U.S. Department of Health and Human Services 200 Independence Avenue, SW Room 509F, HHH Building Washington, D.C. 20201 Website: ocrportal.hhs.gov/ocr/portal/lobby Complaint Form: hhs.gov/ocr/complaints/index

If you or a Passport Member need additional help or more information, call the Office of Civil Rights at (800) 368-1019; TTY/TDD:(800) 537-7697.

Cultural Competency

Passport is committed to reducing Healthcare disparities. Training employees, Providers and their staff and quality monitoring are the cornerstones of successful culturally competent service delivery. Passport integrates cultural competency training into the overall Provider training and quality-monitoring programs. An integrated quality approach enhances the way people think about our Members, service delivery and program development so that cultural competency becomes a part of everyday thinking.

Provider and Community Training

Passport offers educational opportunities in cultural competency concepts for Providers, their staff, and community-based organizations. Passport conducts Provider training during Provider orientation with annual reinforcement training offered through Provider Relations and/or online/web-based training modules. Web-based training modules can be found on Passport's website at https://www.molinahealthcare.com/providers/ky/medicaid/home.aspx.

Training modules, delivered through a variety of methods, include:

1. Provider written communications and resource materials
2. On-site cultural competency training
3. Online cultural competency provider training modules
4. Integration of cultural competency concepts and non-discrimination of service delivery into Provider communications

Integrated Quality Improvement

Passport ensures Member access to language services such as oral interpretation, American Sign Language (ASL) and written translation. Passport must also ensure access to programs, aids and services that are congruent with cultural norms. Passport supports Members with disabilities and assists Members with LEP.

Passport develops Member materials according to Plain Language Guidelines. Members or Providers may also request written Member materials in alternate languages and formats (i.e., Braille, audio, large print), leading to better communication, understanding and Member satisfaction. Online materials found on MolinaHealthcare.com and information delivered in digital form meet Section 508 accessibility requirements to support Members with visual impairments.

Key Member information, including appeal and grievance forms, is also available in threshold languages on the Passport Member website.

Access to Language Services

Providers may request interpreters for Members whose primary language is other than English by calling the Passport Member Contact Center at (800) 578-0775. If Passport Member Contact Center representatives are unable to interpret in the requested language, the representative will immediately connect you and the Member to a qualified language service provider.

Passport Providers must support Member access to telephonic language services by offering a telephone with speaker capability or a telephone with a dual headset. Providers may offer Passport Members interpreter services if the Members do not request them on their own. Please remember it is never permissible to ask a family member, friend or minor to interpret.

All eligible Members with LEP are entitled to receive interpreter services. Pursuant to Title VI of the Civil Rights Act of 1964, services provided for Members with LEP, limited reading proficiency circumstances are Passport Members responsible for the cost of such services. Written procedures are to be maintained by each office or facility regarding their process for obtaining such services. Passport is available to assist providers with locating these services if needed.

An LEP is an individual whose primary language for communication is not English and who individual has a limited ability to read, write, speak, or ~~write~~ understand English well enough to understand and communicate effectively (whether because of language, cognitive or physical limitations). It is possible that an individual with LEP may be able to speak or understand English but still be limited to read or write in English. It is also important to not assume that an individual who speaks some English is proficient in the technical vocabulary of the health care services required.

Passport Members are entitled to:

- Be provided with effective communications with medical Providers as established by the Americans with Disabilities Act of 1990, the Rehabilitation Act of 1973, and the Civil Rights Act of 1964
- Be given access to care managers trained to work with individuals with cognitive impairments
- Be notified by the medical Provider that interpreter services including ASL are available at no cost

- Be given reasonable accommodation, appropriate auxiliary aids and services
- Decide, with the medical Provider, to use an interpreter and receive unbiased interpretation
- Be assured of confidentiality, as follows:
- Interpreters must adhere to Health and Human Service Commission (HHSC) policies and procedures regarding confidentiality of Member records
- Interpreters may, with Member written consent, share information from the Member's records only with appropriate medical professionals and agencies working on the Member's behalf
- Interpreters must ensure that this shared information is similarly safeguarded
- Have interpreters, if needed, during appointments with the Member's Providers and when talking to the health plan

Interpreters include people who can speak the Member's primary language, assist with a disability, or help the Member understand the information.

When Passport Members need an interpreter, limited hearing and/or limited reading services for Healthcare services, the Provider should:

- Verify the Member's eligibility and medical benefits.
- Inform the Member that an interpreter, limited hearing, and/or limited reading services are available.
- Passport is available to assist Providers with locating these services if needed:
    - Providers needing assistance finding on-site video remote, or telephonic interpreter services.
    - Providers needing assistance finding translation services. obtaining written materials in preferred languages
    - Providers with Members who cannot hear or have limited hearing ability may use TTY/TDD at 711.
    - Providers with Members with limited vision may contact Passport for documents in large print, braille or audio version.
    - Providers with Members with limited reading proficiency (LRP).The Passport Member Services representative will verbally explain the information, up to and including reading the documentation to the Members or offer the documents in audio version.

Documentation

As a contracted Passport Provider, your responsibilities for documenting Member language services/needs in the Member's medical record are as follows:

- Record the Member's language preference in a prominent location in the medical record. This information is provided to you on the electronic Member lists that are sent to you each month by Passport.
- Document all Member requests for interpreter services.

- Document who provided the interpreter service. This includes the name of Passport's internal staff or someone from a commercial interpreter service vendor. Information should include the interpreter's name, operator code and vendor.
- Document all counseling and treatment done using interpreter services.
- Document if a Member insists on using a family member, friend or minor as an interpreter or refuses the use of interpreter services after notification of their right to have a qualified interpreter at no cost.

Members Who Are Deaf or Hard of Hearing

TTY/TDD connection is accessible by dialing 711. This connection provides access to the Passport Member and Provider Contact Center, quality, Healthcare services and all other health plan functions.

Passport strongly recommends that Provider offices make assistive listening devices available for Members who are deaf and hard of hearing. Assistive listening devices enhance the sound of the Provider's voice to facilitate a better interaction with the Member.

Passport will provide face-to-face service delivery for ASL to support our Members who are deaf or hard of hearing. Requests should be made at least three (3) business days in advance of an appointment to ensure the availability of the service. In most cases, Members will have made this request via the Passport Member Contact Center.

24-hour Nurse Advice Line

Passport provides a nurse advice line for Members 24 hours per day, 7 days per week. The 24-hour Nurse Advice Line provides access to 24-hour interpretive services. Members may call Passport's 24-hour Nurse Advice Line directly at (800) 606-9880 (English and Spanish), or TTY/TDD 711 for persons with hearing impairments. The 24-hour Nurse Advice Line telephone numbers are also printed on Passport Member ID cards.

Program and Policy Review Guidelines

Passport conducts assessments at regular intervals of the following information to ensure its programs are most effectively meeting the needs of its Members and Providers:

- Annual collection and analysis of race, ethnicity, and language data from:
    - Eligible individuals to identify significant cultural and linguistically diverse populations within a plan's membership.
    - Contracted Providers to assess gaps in network demographics.
- Revalidate data at least annually.
- Local geographic population demographics and trends derived from publicly available sources (Community Health Measures and State Rankings Report).
- Applicable national demographics and trends derived from publicly available sources.
- Assessment of Provider Network and cultural responsiveness.
- Collection of data and reporting for the Diversity Race/Ethnicity Description of Membership

HEDIS® measure.
- Collection of data and reporting for the Language Description of Membership HEDIS® measure
- Annual determination of threshold languages and processes in place to provide Members with vital information in threshold languages.
- Identification of specific cultural and linguistic disparities found across the plan's subpopulations.
- Analysis of HEDIS® and <Consumer Assessment of Healthcare Providers and Systems (CAHPS®) Qualified Health Plan (QHP) Enrollee Experience Survey results for potential cultural and linguistic disparities that prevent Members from obtaining the recommended key chronic and preventive services

CAHPS® is a registered trademark of the Agency for Healthcare Research and Quality (AHRQ).

4. Member Rights and Responsibilities

Providers must comply with the rights and responsibilities of Passport Members as outlined in the Passport Member Handbook and on the Passport Member website.

The Member Handbook that is provided to Members annually is hereby incorporated into this Provider Manual. The most current Member Handbook can be found on the Member pages of Passport's website at https://www.molinahealthcare.com/members/ky/en-us/mem/medicaid/medicaid.aspx.

The most current Member Rights and Responsibilities can be found on the Member pages of Passport's website at https://www.molinahealthcare.com/members/ky/en-us/mem/medicaid/medicaid.aspx.

State and federal law requires that Healthcare Providers and Healthcare facilities recognize Member rights while the Members are receiving medical care and that Members respect the Healthcare Providers or Healthcare facility's right to expect certain behavior on the part of the Members.

For additional information, please contact the Passport Provider Contact Center at (855) 994-2453 Monday through Friday. TTY/TDD: 711 for persons with hearing impairments.

Second Opinions

If Members do not agree with their Provider's plan of care, they have the right to a second opinion from another Provider. Members should call the Passport Member Contact Center to find out how to get a second opinion. Second opinions may require prior authorization.

5. Eligibility, Enrollment, Disenrollment

Enrollment

Enrollment in Medicaid Programs

The Kentucky Department for Medicaid Services has the exclusive right to determine an individual's eligibility for the Medicaid Program and eligibility to become a Passport Member. No eligible Member shall be refused enrollment or re-enrollment, have their enrollment terminated, or be discriminated against in any way because of their health status, need for health services race, ethnicity, national origin, religion, gender, age, mental or physical disability, or sexual orientation.

No eligible Member shall be refused enrollment or re-enrollment, have their enrollment terminated or be discriminated against in any way because of their health status, pre-existing physical or mental condition, including pregnancy, hospitalization, or the need for frequent or high-cost care.

Effective Date of Enrollment

Eligibility begins on the first day of the month for Members joining Passport with the following exceptions:

- Newborns, born to an eligible mother, are eligible at birth
- Members who meet the requirements for presumptive eligibility, in accordance with
- commonwealth and federal guidelines are effective on the of eligibility determination
- Unemployed parent program Members are enrolled beginning the date that the definition
- of unemployment or underemployment, in accordance with 45 D.F.R. 233.100, is met.

Eligibility Verification

Medicaid Programs

The state of Kentucky through the Department for Medicaid Services determines eligibility for the Medicaid programs. Payment for services rendered is based on eligibility and benefit entitlement. The contractual agreement between Providers and Passport places the responsibility for eligibility verification on the Provider of services.

Eligibility Listing for Medicaid Programs

Providers who contract with Passport may verify a Member's eligibility and/or confirm PCD assignment by checking the following:

- Passport Provider Contact Center automated IVR system at (855) 994-2453.

- Eligibility can also be verified through the state at Eligibility can also be verified through the KY HealthNet System at http://kymmis.com/
- SKYGEN portal

Possession of a Passport Member ID Card does not mean a recipient is eligible for Medicaid services. A Provider should verify a recipient's eligibility each time the recipient receives services. The verification sources can be used to verify a recipient's enrollment in a managed care plan. The name and telephone number of the managed care plan are given along with other eligibility information.

Identification Cards

Members are reminded in their Member Handbooks to present Passport Member ID cards when requesting medical or pharmacy services. The Passport Member ID card can be a physical ID card or a digital ID card. It is the Provider's responsibility to ensure Passport Members are eligible for benefits and to verify PCD assignment prior to rendering services. Unless an emergency medical condition exists, Providers may refuse service if the Member cannot produce the proper identification and eligibility cards.

Disenrollment

Voluntary Disenrollment

Passport Members may change to another health plan during their first 90 days after initial enrollment, and annually thereafter.

Voluntary disenrollment does not preclude Members from filing a grievance with Passport for incidents occurring during the time they were covered.

Involuntary Disenrollment

The Department for Medicaid Services has the sole authority to disenroll Members. Disenrollment may be initiated for the following reasons:

- Member commits fraud related to the Medicaid program
- Member is abusive or threatening to Passport, Passport's agents, or Providers
- Member is admitted to a nursing facility for more than 31 days

- Member is incarcerated in a correctional facility
- Member no longer qualifies for Medicaid Assistance
- Member cannot be located

PCD Dismissal

A PCD may dismiss a Member from their practice under following circumstances:

- Incompatibility of the PCP/patient relationship
- Member has not utilized a service within one year of enrollment in the PCP's practice and
- The PCP has documented unsuccessful contact attempts by mail and phone on at least six separate occasions during the year
- Inability to meet the medical needs of the Member.

A PCD may not dismiss a Member from their practice under following circumstances:

- Change in Member's health status or need for treatment
- Member's utilization of medical services
- Member's diminished mental capacity.
- Disruptive behavior that results from the Member's special Healthcare needs unless the
- Behavior impairs the ability of the PCP to furnish services to the Member or others
- Transfer requests shall not be based on race, color, national origin, handicap, age, or gender.
- The initial PCP must serve until the new PCP begins serving the Enrollee, barring ethical or legal issues. The Enrollee has the right to a grievance regarding such a transfer. The PCP shall make the request for change to the Contractor in writing. The Enrollee may request a PCP change in writing, face to face or via telephone

This section does not apply if the Member's behavior is attributable to a physical or behavioral condition.

Missed Appointments

Participating Providers are responsible for establishing a process for documenting missed appointments. When a Member does not keep a scheduled appointment, it is to be noted in the Member's record, and the Provider is to assess if a visit is still medically indicated. All efforts to notify the Member must be documented in the medical record. Providers are strongly encouraged to report missed or cancelled appointments within the Missed or Cancelled Appointments Panel in KY HealthNet (kymmis.com).

6. Benefits and Covered Services

Please visit the KY Department for Medicaid services for a complete list of covered benefits, limitations, prior authorization requirements and fees located here: KY DENTAL BENEFITS. You may also please contact Passport at (855) 994-2453 8 am to 6 pm, Eastern Time.

Member Cost Share

Cost share is the deductible, co-payment, or co-insurance that Members must pay for covered services provided under their Passport plan. The cost share amount Members will be required to pay for each type of covered service is summarized on the Passport Member ID card.

It is the Provider's responsibility to collect the co-payment and other Member cost share from the Member to receive full reimbursement for a service. The amount of the co-payment and other cost share will be deducted from the Passport payment for all Claims involving cost share.

Services Covered by Passport

Passport covers the dental services described on the state website located here: KY DENTAL BENEFITS. You may also contact the Passport Provider Contact Center at (855) 994-2453 8 am to 6 pm, Eastern Time.

Links to Benefit Information

Member benefit materials including the Member Handbook can be found on Passport's website at https://www.molinahealthcare.com/members/ky/en-us/mem/home.aspx

Obtaining Access to Certain Covered Services

Emergency Mental Health or Substance Abuse Disorder Services

Members are directed to call 988, 911 or go to the nearest emergency room if they need emergency mental health or substance use services. Examples of emergency mental health or substance use problems are:

- Danger to self or others
- Not being able to carry out daily activities
- Things that will likely cause death or serious bodily harm

Out-of-Area Emergencies

Members who have a health emergency who cannot get to a Passport approved Provider are directed to do the following:

- Go to the nearest emergency room
- Call the number on the Passport Member ID card
- Call Member's PCD and follow-up within 24 to 48 hours

For out-of-area emergency services, out-of-network Providers are directed to call the Passport contact number on the back of the Passport Member ID card for additional benefit information and may be asked to transfer Members to an in-network facility when the Member is stable.

Emergency Transportation

When a Member's condition is life-threatening and requires the use of special equipment, life support systems and close monitoring by trained attendants while en route to the nearest appropriate facility, emergency transportation is thus required. Emergency transportation includes but is not limited to ambulance, air, or boat transport.

Non-Emergency Medical Transportation

The Kentucky Department for Medicaid Services contracts with the Kentucky Transportation Cabinet, Office of Transportation Delivery's HSTD program to provide non-emergency medical transportation (NEMT). Through the HSTD program, certain eligible Members receive safe and reliable transportation to Medicaid Covered Services. More information about the HSTD program is available at: HSTD.

Passport covers non-emergency transport by stretcher and by ambulance for Members. Only non-emergency Air Ambulance requires prior authorization. Additional information regarding the availability of this benefit is available by contacting Passport Provider Contact Center at (855) 994-2453.

Emergency Services

Emergency Services or Emergency Care means: covered inpatient and outpatient services that are as follows:

- Furnished by a Provider that is qualified to furnish these services; and
- Needed to evaluate or stabilize an Emergency Medical Condition.

Emergency Medical Condition or Emergency means *a* medical condition manifesting itself by acute symptoms of sufficient severity (including severe pain) that a prudent layperson, who possesses an average knowledge of health and medicine, could reasonably expect the absence of immediate medical attention to result in:

Placing the health of the individual (or with respect to a pregnant woman, the health of the woman or her unborn child) in serious jeopardy, Serious impairment of bodily functions, or Serious dysfunction of any bodily organ or port; or with respect to a pregnant woman having contractions:

- That there is an inadequate time to affect a safe transfer to another hospital before delivery, or
- That transfer may pose a threat to the health or safety of the woman or the

unborn child.

Emergent and Urgent Care Services are covered by Passport without an authorization. This includes non-contracted Providers inside or outside of Passport's service area. Immediate treatment for any Emergency Medical or Behavioral Health Services by a health provider that is most suitable for the type of injury, illness, or condition, regardless of whether the facility is in Contractor's Network.

24-hour Nurse Advice Line

Members may call the 24-hour Nurse Advise Line any time they are experiencing symptoms or need Healthcare information. Registered nurses are available 24 hours a day, 7 days a week, 365 days a year.

- English/Spanish Phone: (800) 606-9880
- TTY/TDD: 711 Relay

Passport is committed to helping our Members:

- Prudently use the services of the Provider's office
- Understand how to handle routine health problems at home
- Avoid making non-emergent visits to the emergency room

These registered nurses do not diagnose. They assess symptoms and guide the patient to the most appropriate level of care following specially designed algorithms unique to the 24-hour Nurse Advice Line. The 24-hour Nurse Advice Line may refer to the PCD, a specialist, 911 or the emergency room. By educating patients, it reduces costs and over-utilization on the Healthcare system.

Health Management Programs

Passport offers programs to help our Members and their families manage various health conditions.

For additional information please refer to the **Healthcare Services** section of this Provider Manual.

Telehealth and Telemedicine Services

Passport Members may obtain physical and behavioral health covered services by participating Providers, using telehealth and telemedicine services. Not all participating Providers offer these services. The following additional provisions apply to the use of telehealth and telemedicine services:

- Services must be obtained from a participating Provider.

- Members have the option of receiving PCD services through telehealth. If they choose to use this option, the Member must use a Network Provider who offers telehealth.
- Services are a method of accessing covered services and not a separate benefit.
- Services are not permitted when the Member and Participating Provider are in the same physical location.
- Member cost sharing may apply based on the applicable benefit guide found in the Member Handbook.
- Services must be coded in accordance with applicable reimbursement policies and billing guidelines.
- Rendering Provider must comply with applicable federal and state guidelines for telehealth service delivery.

For additional information on telehealth and telemedicine claims and billing please refer to the **Claims and Compensation** section of this Provider Manual.

7. Healthcare services

Introduction

Healthcare services (HCS) is comprised of utilization management (UM) and care management (CM) departments that work together to achieve an integrated model based upon empirically validated best practices that have demonstrated positive results. Research and experience show that a higher-touch, Member-centric care environment for at-risk Members supports better health outcomes. Passport provides CM services to Members to address a broad spectrum of needs, including chronic conditions that require the coordination and provision of Healthcare services. Elements of the Passport management program include pre-service authorization review, inpatient authorization management that includes pre-admission, admission and concurrent medical necessity review and restrictions on the use of out-of-network or non-participating Providers.

Utilization Management (UM)

Passport ensures the service delivered is medically necessary and demonstrates an appropriate use of resources based on the level of care needed for a Member. This program promotes the provision of quality, cost-effective and medically appropriate services that are offered across a continuum of care as well as integrating a range of services appropriate to meet individual needs. Passport's UM program maintains flexibility to adapt to changes in the Member's condition and is designed to influence a Member's care by:

- Managing available benefits effectively and efficiently while ensuring quality care
- Evaluating the medical necessity and efficiency of Healthcare services across the continuum of care
- Defining the review criteria, information sources and processes that are used to review and approve the provision of items and services, including prescription drugs

- Coordinating, directing, and monitoring the quality and cost effectiveness of Healthcare resource utilization
- Implementing comprehensive processes to monitor and control the utilization of Healthcare resources
- Ensuring services are available in a timely manner, in appropriate settings and are planned, individualized, and measured for effectiveness
- Reviewing processes to ensure care is safe and accessible
- Ensuring qualified Healthcare professionals perform all components of the UM processes
- Ensuring that UM decision making tools are appropriately applied in determining medical necessity decision

Key Functions of the UM Program

All prior authorizations are based on a specific standardized list of services. The key functions of the UM program are listed below.

- **Eligibility and oversight**
  - Eligibility verification
  - Benefit administration and interpretation
  - Verification that authorized care correlates to Member's medical necessity needs(s) and benefit plan
  - Verifying of current Provider/hospital contract status
- **Resource management**
  - Prior authorization and referral management
  - Admission and inpatient review
  - Referrals for discharge planning and care transitions
  - Staff education on consistent application of UM functions
- **Quality Management**
  - Evaluate satisfaction of the UM program using Member and Provider input
  - Utilization data analysis
  - Monitor for possible over- or under-utilization of clinical resources
  - Quality oversight
  - Monitor for adherence to CMS, NCQA, state and health plan UM standards

For more information about Passport's UM program or to obtain a copy of the HCS program description, clinical criteria used for decision making and how to contact a UM reviewer, access the Passport website or contact the UM department.

Providers and delegated entities who assume responsibility for UM must adhere to Passport's UM Policies. Their programs, policies and supporting documentation are reviewed by Passport at least annually.

UM Decisions

An organizational determination is any decision made by Passport or other delegated entity with respect to the following:

- Determination to authorize, provide or pay for services (favorable determination)
- Determination to delay, modify or deny authorization or payment of request (adverse determination).

Passport follows a hierarchy of medical necessity decision making with federal and state regulations taking precedence. Passport covers all services and items required by state and federal regulations.

Board-certified licensed reviewers from appropriate specialty areas are utilized to assist in making determinations of medical necessity, as appropriate. All utilization determinations are made in a timely manner to accommodate the clinical urgency of the situation, in accordance with federal and state regulatory requirements and NCQA standards.

Requests for authorization not meeting medical necessity criteria are reviewed by a designated Passport Dental director or other appropriate clinical professional. Only a licensed Provider or pharmacist, doctoral-level clinical psychologist, or certified addiction medicine specialist, as appropriate, may determine to delay, modify, or deny authorization of services to a Member.

Providers can contact Passport's Healthcare Services department at (800) 578-0775 to obtain Passport's UM Criteria.

Where applicable, Passport clinical policies can be found on the public website at MolinaClinicalPolicy.com. Please note that passport follows state-specific criteria, if available, before applying Passport-specific criteria.

Medical Necessity

This is for the purpose of preventing, evaluating, diagnosing, or treating an illness, injury, disease, or its symptoms. Those services must be deemed by Passport to be:

1. In accordance with generally accepted standards of medical practice.
2. Clinically appropriate and clinically significant, in terms of type, frequency, extent, site and duration. They are considered effective for the patient's illness, injury, or disease.
3. Not primarily for the convenience of the patient, or other Healthcare Provider. The services must not be more costly than an alternative service or sequence of services at least as likely to produce equivalent therapeutic or diagnostic results as to the diagnosis or treatment of that patient's illness, injury, or disease.

For these purposes, "generally accepted standards of medical practice" means standards that are based on credible scientific evidence published in peer-reviewed medical literature. This literature is generally recognized by the relevant medical community, Provider specialty society

recommendations, the views of Providers practicing in relevant clinical areas and any other relevant factors.

The fact that a Provider has prescribed, recommended, or approved medical or allied goods or services does not, by itself, make such care, goods or services medically necessary, a medical necessity or a covered service/benefit.

Medical Necessity Review

Passport only reimburses for services that are medically necessary. Medical necessity review may take place prospectively, as part of the inpatient admission notification/concurrent review or retrospectively. To determine medical necessity, in conjunction with independent professional medical judgment, Passport uses nationally recognized evidence-based guidelines, third party guidelines, CMS guidelines, state guidelines, Passport clinical policies, guidelines from recognized professional societies and advice from authoritative review articles and textbooks.

Levels of Administrative and Clinical Review

The Passport review process begins with administrative review followed by clinical review if appropriate. Administrative review includes verifying eligibility, appropriate vendor or Participating Provider and benefit coverage. The Clinical review includes medical necessity and level of care.

All UM requests that may lead to a medical necessity adverse determination are reviewed by a Healthcare professional at Passport (Dental director, pharmacy director or appropriately licensed Healthcare professional).

Passport's Provider training includes information on the UM processes and authorization requirements.

Clinical Information

Passport requires copies of clinical information to be submitted for documentation. Clinical information includes but is not limited to Provider emergency department notes, inpatient history/physical exams, discharge summaries, Provider progress notes, Provider office notes, Provider orders, nursing notes, results of laboratory or imaging studies, therapy evaluations and therapist notes. Passport does not accept clinical summaries, telephone summaries or inpatient case manager criteria reviews as meeting the clinical information requirements unless state or federal regulations allows such documentation to be acceptable.

Prior Authorization

Passport requires prior authorization for specified services if the requirement complies with federal or state regulations and the Provider Agreement with Passport. The list of services that require prior authorization is available in narrative form, along with a more detailed list by

Current Procedural Terminology (CDT®) and Healthcare Common Procedural Coding System (HCPCS) codes here: KY DENTAL BENEFITS.

CDT® is a registered trademark of the American Dental Association.

Peer-to-Peer Review

Upon receipt of an adverse determination, the Provider (peer) may request a peer-to-peer discussion within five (5) business days from the notification.

A "peer" is considered the Member's or Provider's clinical representative (licensed Dental professional). Contracted external parties, administrators or facility UM staff can only request that a peer-to-peer telephone communication be arranged and performed but the discussion should be performed by a peer.

When requesting a peer-to-peer discussion, please be prepared with the following information:

- Member name and Passport Member ID number
- Authorization ID number
- Requesting Provider name, contact number and best times to call

If a Dental director is not immediately available, the call will be returned within two (2) business days. Every effort will be made to return calls as expeditiously as possible.

Requesting Prior Authorization

Notwithstanding any provision in the Provider Agreement with Passport that requires the Provider to obtain prior authorization directly from Passport, Passport may choose to contract with external vendors to help manage prior authorization requests.

SKYGEN portal: Participating Providers are encouraged to use the SKYGEN portal for prior authorization submissions whenever possible. Instructions for how to submit a prior authorization request are available on the SKYGEN portal. The benefits of submitting your prior authorization request through the SKYGEN portal are:

- Create and submit prior authorization requests
- Check status of prior authorization requests
- Receive notification of change in status of prior authorization requests
- Attach medical documentation required for timely medical review and decision-making

Open Communication about Treatment

Passport prohibits contracted Providers from limiting Provider or Member communication regarding a Member's Healthcare. Providers may freely communicate with and act as an advocate for their patients. Passport requires provisions within Provider contracts that prohibit

solicitation of Members for alternative coverage arrangements for the primary purpose of securing financial gain. No communication regarding treatment options may be represented or construed to expand or revise the scope of benefits under a health plan or insurance contract.

Passport and its contracted Providers may not enter contracts that interfere with any ethical responsibility or legal right of Providers to discuss information with a Member about the Member's Healthcare. This includes, but is not limited to, treatment options, alternative plans, or other coverage arrangements.

Delegated Utilization Management Functions

Passport may delegate UM functions to qualifying Providers and delegated entities. These entities must be able to perform the delegated activities and maintain specific delegation criteria in compliance with all current Passport policies and regulatory and certification requirements. For more information about delegated UM functions and the oversight of such delegation, please refer to the **Delegation** section of this Provider Manual.

Emergency Services

A medical screening exam performed by licensed medical personnel in the emergency department and subsequent emergency services rendered to the Member do not require prior authorization from Passport.

Emergency services are covered on a 24-hour basis without the need for prior authorization for all Members experiencing an emergency medical condition.

Post-stabilization care services are covered services that are:

- Related to an emergency medical condition
- Provided after the Member is stabilized
- Provided to maintain the stabilized condition or under certain circumstances, to improve or resolve the Member's condition

Passport also provides Members with a 24-hour Nurse Advice Line for medical advice. The 911 information is given to all Members at the onset of any call to the plan.

For Members within our service area, Passport contracts with vendors that provide 24-hour emergency services for ambulance and hospitals. An out-of-network emergency hospital stay may only be covered until the Member has stabilized sufficiently to transfer to an available participating facility. Services provided after stabilization in a non-participating facility may not be covered and the Member may be responsible for payment.

Passport care managers will contact Members over-utilizing the emergency department to provide assistance whenever possible and determine the reason for using emergency services.

Care managers will also contact the PCD to ensure that Members are not accessing the emergency department because of an inability to be seen by the PCD.

Post-Service Review

Failure to obtain prior authorization when required may result in denial of payment for those services. The only possible exception for payment because of post-service review is if information is received indicating the Provider did not know, nor could have known, that the patient was a Passport Member or there was a Passport error. In those cases, a medical necessity review will be performed. Decisions, in this circumstance, will be based on medical necessity.

Specific federal or state requirements or Provider contracts that prohibit administrative denials supersede this policy.

Affirmative Statement about Incentives

All medical decisions are coordinated and rendered by qualified Practitioners and licensed staff unhindered by fiscal or administrative concerns. Passport and its delegated contractors do not use incentive arrangements to reward the restriction of medical care to Members.

Passport requires that all utilization-related decisions regarding Member coverage and/or services are based solely on the appropriateness of care and existence of coverage. Passport does not specifically reward Practitioners or other individuals for issuing denials of coverage or care. Passport does not receive financial incentives or other types of compensation to encourage decisions that result in underutilization.

Out-of-Network Providers and Services

Passport maintains a contracted network of qualified Healthcare professionals who have undergone a comprehensive credentialing process to provide medical care to Passport Members. Passport requires Members to receive medical care within the participating, contracted network of Providers unless it is for emergency services as defined by federal law. If there is a need to go to a non-contracted Provider, all care provided by non-contracted, non-network Providers must be prior authorized by Passport. Non-network Providers may provide emergency services for a Member who is temporarily outside the service area without prior authorization or as otherwise required by federal or state laws or regulations.

Avoiding Conflict of Interest

The HCS department affirms its decision-making is based on the appropriateness of care and service and the existence of benefit coverage.

Passport does not reward Providers or other individuals for issuing denials of coverage or care. Furthermore, Passport never provides financial incentives to encourage authorization decision

makers to make determinations that result in under-utilization. Passport also requires our delegated Providers to avoid this kind of conflict of interest.

Coordination of Care and Services

Passport HCS staff work with Providers to assist with coordinating referrals, services and benefits for Members who have been identified for Passport's Integrated Care Management (ICM) program via assessment or referral such as, self-referral, Provider referral, etc. In addition, the coordination of care process assists Passport Members, as necessary, in transitioning to other care when benefits end.

Passport staff provide an integrated approach to care needs by assisting Members with identification of resources available to the Member, such as community programs, national support groups, appropriate specialists, and facilities, identifying best practice or new and innovative approaches to care. Care coordination by Passport staff is done in partnership with Providers, Members, and/or their authorized representative(s) to ensure efforts are efficient and non-duplicative.

Continuity and Coordination of Provider Communication

Passport stresses the importance of timely communication between Providers involved in a Member's care. This is especially critical between specialists, including behavioral health Providers and the Member's PCD. Information should be shared in such a manner as to facilitate communication of urgent needs or significant findings.

Reporting of Suspected Abuse and/or Neglect

A vulnerable adult is a person who is receiving or may be in need of receiving community care services by reason of mental or other disability, age, or illness; and who is or may be unable to take care of themself or unable to protect themself against significant harm or exploitation. When working with children one may encounter situations suggesting abuse, neglect, and/or unsafe living environments.

Every person who knows or has reasonable suspicion that a child or adult is being abused or neglected must report the matter immediately. Specific professionals mentioned under the law as mandated reporters are:

- Physicians, dentists, interns, residents, or nurses
- Public or private school employees or child caregivers
- Psychologists, social workers, family protection workers or family protection specialists
- Attorneys, ministers, or law enforcement officers

Suspected abuse and/or neglect should be reported as follows:

Child Abuse

Suspected child abuse should be reported to the Child Protection Branch of the Kentucky Cabinet for Health and Family Services (CHFS). To report suspected child abuse and neglect, call toll-free: 877-KYSAFE1 (877-597-2331) (800) 752-6200. Non-emergency reports can be made online. https://prd.webapps.chfs.ky.gov/reportabuse/OutofHours.aspx. If the child's life is in danger, call 911.

Adult Abuse

Suspected abuse or neglect of an adult should be reported to the Adult Protection branch of

- CHFS. Non-emergency reports should be made online using the Kentucky Child/Adult Protective Services Reporting System at: https://prd.webapps.chfs.ky.gov/reportabuse/OutofHours.aspx.
- If the situation is a life-threatening emergency, call 911.

Member Newsletters

Member newsletters are posted on the MolinaHealthcare.com website at least once a year. The articles are about topics asked by Members. The tips are aimed to help Members stay healthy.

Member Health Education Materials

Members can access our easy-to-read evidence-based educational materials about nutrition, preventive services guidelines, stress management, exercise, cholesterol management, asthma, diabetes, depression, and other relevant health topics identified during our engagement with Members. Materials are available through the Member Portal, direct mail as requested, email and the My Passport mobile app.

Program Eligibility Criteria and Referral Source

HM programs are designed for Passport Members with a confirmed diagnosis. Identified Members will receive targeted outreach such as educational materials, telephonic outreach, or other materials to access information on their condition. Members can contact Passport Member Services at any time and request to be removed from the program.

Members may be identified for or referred to HM programs from multiple pathways which may include the following:

- Pharmacy Claims data for all classifications of medications.
- Encounter Data or paid Claims with a relevant CMS-accepted diagnosis or procedure code.
- Member Services welcome calls made by staff to new Member households and incoming Member calls have the potential to identify eligible program participants. Eligible Members are referred to the program registry.
- Member assessment calls made by staff for the initial HRA for newly enrolled Members.

- External referrals from Provider(s), caregivers, or community-based organizations.
- Internal referrals from 24-hour Nurse Advice Line, medication management or utilization management.
- Member self-referral due to general plan promotion of program through Member newsletter or other Member communications.

Provider Participation

Provider resources and services may include:

- Annual Provider feedback letters containing a list of patients identified with the relevant disease
- Clinical resources such as patient assessment forms and diagnostic tools
- Patient education resources
- Provider Newsletters promoting the health management programs, including how to enroll patients and outcomes of the programs.
- Clinical Practice Guidelines
- Preventive Health Guidelines
- Case management collaboration with the Member's Provider
- Faxing a Provider Collaboration Form to the Member's Provider when indicated

Additional information on health management programs is available from your local Passport HCS department.

Primary Care Dental (PCD) Providers

Passport provides a panel of PCDs to care for its Members.

Specialty Providers

Passport maintains a network of specialty Providers to care for its Members.

Passport will help to arrange specialty care outside the network when Providers are unavailable, or the network is inadequate to meet a Member's Dental needs. To obtain such assistance contact the Passport UM department. Referrals to specialty care outside the network require prior authorization from Passport.

Care Management (CM)

Passport provides a comprehensive ICM program to all Members who meet the criteria for services. The ICM program focuses on coordinating the care, services and resources needed by Members throughout the continuum of care. Passport adheres to Case Management Society of America Standards of Practice Guidelines in its execution of the program.

The Passport care managers may be licensed professionals and are educated, trained, and experienced in Passport's ICM program. The ICM program is based on a Member advocacy philosophy, designed and administered to assure the Member value-added coordination of

healthcare and services, to increase continuity and efficiency and to produce optimal outcomes. The ICM program is individualized to accommodate a Member's needs with collaboration and input from the Member's PCD. The Passport care manager will complete an assessment with the Member upon engagement after identification for ICM enrollment, assist with arrangement of individual services for Members whose needs include ongoing medical care, home Healthcare, rehabilitation services and preventive services. The Passport care manager is responsible for assessing the Member's appropriateness for the ICM program and for notifying the PCD of ICM program enrollment, as well as facilitating and assisting with the development of the Member's ICP.

8. Quality

Maintaining Quality Improvement Processes and Programs

Passport works with Members and Providers to maintain a comprehensive Quality Improvement (QI) program. You can contact the Passport Quality department at (800) 578-0775.

The address for mail requests is:

Passport by Molina Healthcare, Inc.
Attn: Quality Department
2028 W. Broadway
Louisville, KY 40203

This Provider Manual contains excerpts from the Passport QI program. For a complete copy of Passport's QI program, you can contact your Provider Relations representative or call the telephone number above to receive a written copy.

Passport has established a QI program that complies with regulatory requirements and accreditation standards. The QI program provides structure and outlines specific activities designed to improve the care, service, and health of our Members. In our QI program description, we describe our program governance, scope, goals, measurable objectives, structure, and responsibilities.

Passport does not delegate quality improvement activities to dental providers. However, Passport requires contracted Providers to comply with the following core elements and standards of care. Passport Providers must:

- Have a quality improvement program in place
- Comply with and participate in Passport's QI program including reporting of access and availability survey and activity results and provision of medical records as part of the HEDIS® review process and during potential quality of care and/or critical incident investigations
- Cooperate with Passport's quality improvement activities that are designed to improve quality of care and services and Member experience

- Allow Passport to collect, use and evaluate data related to Provider performance for quality improvement activities, including but not limited to focus areas, such as clinical care, care coordination and management, service, access, and availability
- Allow access to Passport quality personnel for site and medical record review processes

Patient Safety Program

Passport's Patient Safety Program identifies appropriate safety projects and error avoidance for Passport Members in collaboration with their PCDs. Passport continues to support safe health practices for our Members through our safety program, pharmaceutical management and care management/health management programs and education. Passport monitors nationally recognized quality index ratings for facilities including adverse events and hospital-acquired conditions as part of a national strategy to improve Healthcare quality mandated by the Patient Protection and Affordable Care Act (ACA) and the Department of Health and Human Services (HHS) to identify areas that have the potential for improving Healthcare quality to reduce the incidence of events.

Quality of Care

Passport has established a systematic process to identify, investigate, review, and report any quality of care, adverse event/never event, critical incident (as applicable) and/or service issues affecting Member care. Passport will research, resolve, track, and trend issues. Confirmed adverse events/never events are reportable when related to an error in medical care that is clearly identifiable, preventable and/or found to have caused serious injury or death to a patient. Passport is not required to pay for inpatient care related to "never events."

Dental Records

Passport requires that dental records be maintained in a manner that is current, detailed, and organized to ensure that care rendered to Members is consistently documented (hard copy or electronic) and that necessary information is readily available in the dental record in accordance with Passport by Molina Healthcare policies and procedures. All entries will be indelibly added to the Member's record. A Member's dental record is the property of the provider who generates the record. PCDs should maintain the following dental record components that include but are not limited to:

- Medical record confidentiality and release of dental records within medical and behavioral Healthcare records.
- Each Member is entitled to a copy of their dental record at no cost.
- Upon notification of transferring Members, Passport will ensure their dental records or copies of dental records are forwarded to the new PCD within ten (10) business days from receipt of the request for transfer of the dental records.
- Passport by Molina Healthcare is not required to obtain written approval from a member before requesting the Member's dental record from the PCD or any other organization or agency.

- Passport by Molina Healthcare must afford Medicaid access to all Members' dental records, whether electronic or paper, in the form, manner, and deadline directed by Passport.
- Medical record content and documentation standards include legibility, accuracy, and plan of care that comply with applicable law and Passport written standards.
- Storage maintenance and disposal processes.
- Process for archiving dental records and implementing improvement activities.
- If care has not been established, information may be kept temporarily in an appropriately labeled file, in lieu of a permanent dental record.
- The temporary file must be associated with the Member's dental record as soon as one is established.

Information related to fraud and abuse may be released. However, HIV-related information may not be disclosed except as provided in state statute, and substance use disorder information shall only be disclosed consistent with Federal and State law including, but not limited to 42 CFR § 2.1 et seq.

Dental Record Keeping Practices

Below is a list of the minimum items that are necessary in the maintenance of the Member's Dental records:

- Each patient has a separate record.
- All records are to be in a locked secure environment
- Records are available at each visit and archived records are available within 24 hours.
- If its hard copy, pages are securely attached in the dental record and records are organized by dividers or color-coded when thickness of the record dictates.
- If electronic, all those with access have individual passwords.
- Record keeping is monitored for Quality and HIPAA compliance.
- Storage maintenance for the determined timeline and disposal per record management processes.
- Process for archiving dental records and implementing improvement activities.
- Records are kept confidential and there is a process for release of dental records.

Dental Record Content

Providers must remain consistent in their practices with Passport's dental record documentation guidelines. Medical records are maintained and should include the following information:

- Each page in the record contains the patient's name or ID number. Member name, date of birth, gender, legal guardianship (if applicable), marital status, address, employer, home and work telephone numbers, and emergency contact. Primary language spoken by the Member and any translation needs. Legible signatures and credentials of

Provider and other staff members within a paper chart. All Providers who participate in the Member's care.

The primary care dentist is responsible for documenting all services provided directly by the PCD. This includes all ancillary and diagnostic services ordered by the PCD, and all diagnostic and therapeutic services for which the member was referred by the PCD. At a minimum, each dental record must contain the following:

- Member demographics: Member name, member ID number, date of birth, gender, marital status, address, employer, home and work telephone numbers, emergency contact information, primary language, and translation needs.
- Legible signature and credentials of provider and other staff members if a paper dental record; after each entry into progress notes. Process notes should include:
  - Review of medical history.
  - Exam findings and diagnosis
  - Verbal or written informed consent.
  - Date of Service
  - Services performed including:
  - Tooth number.
  - Arch.
  - Surfaces.
  - Quadrant.
  - Summary of the appointment and discussions with the member
  - Review treatment for the next visit as applicable
  - Presenting complaints, diagnoses, and treatment plans, including follow-up visits and referrals to other providers.
  - Prescribed medications, including dosages and dates of initial or refill prescriptions.
  - Allergies and adverse reactions (or notation that none are known).
  - Treatment plans are consistent with diagnosis.
  - A working diagnosis is recorded with the clinical findings.
  - Progress notes clearly and thoroughly state the intent on all ordered services and treatments.
  - There are notations regarding follow-up care, calls, or visits, including the next preventative care visit when appropriate.
  - Notes from consultants are in the record if applicable.
  - All staff and provider notes are signed physically or electronically with either name or initials.
  - All entries are dated.
  - All ancillary services reports.

Dental Record Organization

- The dental record is legible to someone other than the writer.

- Each patient has an individual record.
- Chart pages are bound, clipped, or attached to the file.
- Chart sections are easily recognized for retrieval of information.
- A release document for each Member authorizing Passport to release dental information for facilitation of dental care.

Dental Record Retrieval

- The dental record is available to the Provider at each encounter.
- The dental record is available to Passport for purposes of Quality Improvement.
- The dental record is available to the applicable State and/or Federal agency and the External Quality Review Organization upon request.
- The dental record is available to the Member at their request at no cost.
- A storage system for inactive Member dental records which allows retrieval within 24 hours, is consistent with State and Federal requirements, and the record is maintained for not less than 10 years from the last date of treatment or for a minor, one year past their 20th birthday but, never less than 10 years.
- An established and functional data recovery procedure in the event of data loss.

Confidentiality

Passport Providers shall develop and implement confidentiality procedures to guard Member protected health information, in accordance with HIPAA privacy standards and all other applicable Federal and State regulations. This should include, and is not limited to, the following:

- Ensure that dental information is released only in accordance with applicable Federal or State Law in pursuant to court orders or subpoenas.
- Maintain records and information in an accurate and timely manner.
- Ensure timely access by Members to the records and information that pertain to them.
- Abide by all Federal and State Laws regarding confidentiality and disclosure of dental records or other health and enrollment information.
- Medical Records are protected from unauthorized access.
- Access to computerized confidential information is restricted.
- Precautions are taken to prevent inadvertent or unnecessary disclosure of protected health information.

Education and training for all staff on handling and maintaining protected Healthcare information.

Additional information on dental records is available from your local Passport Quality department. For additional information regarding HIPAA please, refer to the Compliance section of this Dental Provider Manual.

Access to Care

Passport maintains access to care standards and processes for ongoing monitoring of access to Healthcare provided by contracted PCDs and participating specialists. Providers surveyed include PCDs (family/general practice, internal medicine and pediatric), OB/GYN (high-volume specialists), Oncologist (high-impact specialists) and behavioral health Providers. Providers are required to conform to the access to care appointment standards listed below to ensure that Healthcare services are provided in a timely manner. The PCD or their designee must be available 24 hours a day, 7 days a week to Members.

Appointment Access

All Providers who oversee the Member's Healthcare are responsible for providing the following appointments to Passport Members in the timeframes noted.

Dental Appointment Timeframe Requirements

Appointment type	Standard
Routine	Within 30 days of the member's request
Emergent	Within 24 hours of the member request
Urgent Care	Within 48 hours of the member's request

Emergency Dental Condition – a dental or oral condition that requires immediate service for relief of symptoms and stabilization of the condition; such conditions include severe pain, hemorrhage, acute infection, traumatic injury to the teeth and surrounding tissue, or unusual swelling of the face or gums.

Emergency Dental Services – those services necessary for the treatment of any condition requiring immediate attention for the relief of pain, hemorrhage, acute infection, or traumatic injury to the teeth, supporting structure (periodontal membrane, Gingival, alveolar bone), jaws, and tissues of the oral cavity.

Urgent Care – those problems, which, though not life threatening, could result in serious injury or disability unless attention is received or do substantially restrict a member's activity.

Additional information on appointment access standards is available from your local Passport Quality department.

After Hours

All Providers must have backup (on-call) coverage after hours or during the Provider's absence or unavailability. Passport requires Providers to maintain a 24-hour telephone service, 7 days a week. This access may be through an answering service or a recorded message after office hours. The service or recorded message should instruct Members with an emergency to hang

up and call 911 or go immediately to the nearest emergency room. Voicemail alone after hours is not acceptable.

Appointment Scheduling

Each Provider must implement an appointment scheduling system. The following are the minimum standards:

1. The Provider must have an adequate telephone system to handle patient volume. Appointment intervals between patients should be based on the type of service provided and a policy defining required intervals for services. Flexibility in scheduling is needed to allow for urgent walk-in appointments.
2. A process for documenting missed appointments must be established. When a Member does not keep a scheduled appointment, it is to be noted in the Member's record, and the Provider is to assess if a visit is still medically indicated. All efforts to notify the Member must be documented in the medical record.
3. When the Provider must cancel a scheduled appointment, the Member is given the option of seeing an associate or having the next available appointment time.
4. Special needs of Members must be met when scheduling appointments. This includes but is not limited to wheelchair-using Members and Members requiring language interpretation.
5. A process for Member notification of preventive care appointments must be established. This includes but is not limited to immunizations and mammograms.
6. A process must be established for Member recall in the case of missed appointments for a condition which requires treatment, abnormal diagnostic test results or the scheduling of procedures which must be performed prior to the next visit.

In applying the standards listed above, participating Providers have agreed that they will not discriminate against any Member on the basis of age, race, creed, color, religion, sex, national origin, sexual orientation, marital status, physical, mental or sensory handicap, gender identity, pregnancy, sex stereotyping, place of residence, socioeconomic status or status as a recipient of Medicaid benefits. Additionally, a participating Provider may not limit their practice because of a Member's medical (physical or mental) condition or the expectation for the need of frequent or high-cost care. If a PCD chooses to close their panel to new Members, Passport must receive 30 calendar day advance written notice from the Provider.

Monitoring Access for Compliance with Standards

Access to care standards are reviewed, revised as necessary and approved by the Quality Improvement and Health Equity Transformation Committee on an annual basis.

Provider network adherence to access standards is monitored via one or more of the following mechanisms:

1. Provider access studies – Provider office assessment of appointment availability, after-hours access, Provider ratios and geographic access.

2. Member complaint data – assessment of Member complaints related to access and availability of care.
3. Member satisfaction survey – evaluation of Members' self-reported satisfaction with appointment and after-hours access.

Analysis of access data includes assessment of performance against established standards, review of trends over time and identification of barriers. Results of the analysis are reported to the Quality Improvement and Health Equity Transformation Committee at least annually for review and determination of opportunities for improvement. Corrective actions are initiated when performance goals are not met and for identified provider-specific and/or organizational trends. Performance goals are reviewed and approved annually by the Quality Improvement and Health Equity Transformation Committee.

Quality of Provider Office Sites

Passport Providers are to maintain office-site and medical record keeping practices standards. Passport continually monitors Member appeals and complaints/grievances for all office sites to determine the need for an office site visit and will conduct office site visits as needed. Passport assesses the quality, safety, and accessibility of office sites where care is delivered against standards and thresholds. A standard survey form is completed at the time of each visit. This includes an assessment of:

- Physical accessibility
- Physical appearance
- Adequacy of waiting and examining room space

Physical Accessibility

Passport evaluates office sites as applicable to ensure that Members have safe and appropriate access to the office site. This includes, but is not limited to, ease of entry into the building, accessibility of space within the office site and ease of access for patients with physical disabilities.

Physical Appearance

The site visits include, but are not limited to, an evaluation of office site cleanliness, appropriateness of lighting and patient safety as needed.

Adequacy of Waiting and Examining Room Space

During the site visit as required, Passport assesses waiting and examining room spaces to ensure that the office offers appropriate accommodations to Members. The evaluation includes but is not limited to appropriate seating in the waiting room areas and availability of exam tables in exam rooms.

Administration and Confidentiality of Facilities

Facilities contracted with Passport must demonstrate overall compliance with the guidelines listed below:

- Office appearance demonstrates that housekeeping and maintenance are performed appropriately on a regular basis, the waiting room is well-lit, office hours are posted, and the parking area and walkways demonstrate appropriate maintenance.
- Accessible parking is available; the building and exam rooms are accessible with an incline ramp or flat entryway, and the restroom is accessible with a bathroom grab bar.
- Adequate seating includes space for an average number of patients in an hour and there is a minimum of two (2) office exam rooms per Provider.
- Basic emergency equipment is in an easily accessible area. This includes a pocket mask and Epinephrine, plus any other medications appropriate to the practice.
- At least one (1) CPR-certified employee is available.
- Yearly Occupational Safety and Health Administration (OSHA) training (fire, safety, blood-borne pathogens, etc.) is documented for offices with 10 or more employees.
- A container for sharps is in each room where injections are given.
- Labeled containers, policies, contracts, and evidence of a hazardous waste management system in place.
- Patient check-in systems are confidential. Signatures on fee slips, separate forms, stickers, or labels are possible alternative methods.
- Confidential information is discussed away from patients. When reception areas are unprotected by sound barriers, scheduling and triage phones are best placed at another location.
- Medical records are stored away from patient areas. Record rooms and/or file cabinets are preferably locked.
- A Clinical Laboratory Improvement Amendment (CLIA) waiver is displayed when the appropriate lab work is run in the office.
- Prescription pads are not kept in exam rooms.
- Narcotics are locked, preferably double-locked. Medication and sample access is restricted.
- System in place to ensure expired sample medications are not dispensed and injectables and emergency medication are checked monthly for outdates.
- Drug refrigerator temperatures are documented daily.

Early and Periodic Screening, Diagnostic and Treatment (EPSDT) Services to Enrollees under 21 years of age

Passport maintains systematic and robust monitoring mechanisms to ensure all required EPSDT services to Enrollees under 21 years of age are timely according to required preventive guidelines. All Enrollees under 21 years of age should receive preventive, diagnostic and treatment services at intervals as set forth in Section 1905 (R) of the Social Security Act. Passport's Quality or the Provider Relations department are also available to perform Provider

training to ensure that best practice guidelines are followed in relation to well-child services and care for acute and chronic Healthcare needs.

Monitoring for Compliance with Standards

Passport monitors compliance with the established performance standards as outlined above at least annually. Performance below Passport's standards may result in a corrective action plan (CAP) with a request that the Provider submit a written CAP to Passport within 30 calendar days. Follow-up to ensure resolution is conducted at regular intervals until compliance is achieved. The information and any response made by the Provider are included in the Provider's permanent credentials file. If compliance is not attained at follow-up, an updated CAP will be required. Providers who do not submit a CAP may be terminated from network participation or closed to new Members.

Quality Improvement Activities and Programs

Passport maintains an active QI program. The QI program provides structure and key processes to carry out our ongoing commitment to the improvement of care and service. Passport focuses on reducing Healthcare disparities through the QI program. The goals identified are based on an evaluation of programs and services, regulatory, contractual and accreditation requirements and strategic planning initiatives.

Health Management and Care Management

The Passport health management and care management programs provide for the identification, assessment, stratification, and implementation of appropriate interventions for members with chronic diseases.

For additional information please refer to the Health Management and Care Management headings in the **Healthcare Services** section of this Provider Manual.

Clinical Practice Guidelines

Passport adopts and disseminates clinical practice guidelines (CPG) to reduce inter-Provider variation in diagnosis and treatment. CPG adherence is measured at least annually. All guidelines are based on scientific evidence, review of medical literature and/or appropriately established authority.

Preventive Health Guidelines

Passport provides coverage of diagnostic preventive procedures based on recommendations published by the U.S. Preventive Services Task Force (USPSTF), Bright Futures/American Academy of Pediatrics and the Centers for Disease Control and Prevention (CDC) in accordance with CMS guidelines. Diagnostic preventive procedures include but are not limited to:

- Adult Preventive Services Recommendations (U.S. Preventive Services Task Force). Links to current recommendations are included on Passport's website.
- Recommendations for Preventive Pediatric Healthcare (Bright Futures/American Academy of Pediatrics). Links to current recommendations are included on Passport's website.
- Recommended Adult Immunization Schedule for ages 19 Years or Older (United States). These recommendations are revised every year by the CDC. Links to current recommendations are included on Passport's website.
- Recommended Child and Adolescent Immunization Schedule for ages 18 years or younger (United States). These recommendations are revised every year by the CDC. Links to current recommendations are included on Passport's website.
- All preventive health guidelines are updated at least annually and more frequently as needed when clinical evidence changes and are approved by the Quality Improvement and Health Equity Transformation Committee. A review is conducted at least monthly to identify new additions or modifications. On an annual basis or when changes are made during the year preventive health guidelines are distributed to Providers at MolinaHealthcare.com and the Provider Manual. Notification of the availability of the preventive health guidelines is published in the Passport Provider Newsletter.

Cultural and Linguistic Appropriate Services

Passport works to ensure all Members receive culturally linguistically appropriate care across the service continuum to reduce health disparities and improve health outcomes. For additional information about Passport's program and services, please refer to the Culturally Linguistically Appropriate Services section of this Provider Manual.

Measurement of Clinical and Service Quality

Passport monitors and evaluates the quality of care and services provided to Members through the following mechanisms:

- HEDIS®
- CAHPS®
- Provider satisfaction survey
- Effectiveness of quality improvement initiatives

Passport evaluates continuous performance according to or in comparison with objectives, measurable performance standards and benchmarks at the national, regional and/or at the local/health plan level.

Contracted Providers and Facilities must allow Passport to use its performance data collected in accordance with the Provider's or facility's contract. The use of performance data may include, but is not limited to, the following: (1) development of Quality Improvement activities; (2) public reporting to consumers; (3) preferred status designation in the network; (4) and/or reduced Member cost sharing.

Passport's most recent results can be obtained from your local Passport Quality department or by visiting our website at www.passporthealthplan.com.

HEDIS®

Passport utilizes NCQA HEDIS® as a measurement tool to provide a fair and accurate assessment of specific aspects of managed care organization performance. HEDIS® is an annual activity conducted in the spring. The data comes from on-site medical record review and available administrative data. All reported measures must follow rigorous specifications and are externally audited to ensure continuity and comparability of results. The HEDIS® measurement set currently includes a variety of Healthcare aspects including immunizations, women's health screening, diabetes care, well check-ups, medication use and cardiovascular disease.

HEDIS® results are used in a variety of ways. The results are used to evaluate the effectiveness of multiple quality improvement activities and clinical programs. The standards are based on established clinical guidelines and protocols, providing a firm foundation to measure the effectiveness of these programs.

Selected HEDIS® results are provided to federal and state regulatory agencies and accreditation organizations. The data are also used to compare against established health plan performance benchmarks.

CAHPS®

CAHPS® is the tool used by Passport to summarize Member satisfaction with Providers, Healthcare and service they receive. CAHPS® examines specific measures, including Getting Needed Care, Getting Care Quickly, How Well Doctors Communicate, Coordination of Care, Customer Service, Rating of Healthcare and Getting Needed Prescription Drugs (for Medicare). The CAHPS® survey is administered annually in the spring to randomly selected Members by an NCQA-certified vendor.

CAHPS® results are used in much the same way as HEDIS® results, only the focus is on the service aspect of care rather than clinical activities. They form the basis for several of Passport's quality improvement activities and are used by external agencies to help ascertain the quality of services being delivered.

Provider Satisfaction Survey

Recognizing that HEDIS® and CAHPS® both focus on Member experience with Healthcare Providers and health plans, Passport conducts a Provider Satisfaction Survey annually. The results from this survey are important to Passport, as this is one of the primary methods used to identify improvement areas pertaining to the Passport Provider network. The survey results have helped establish improvement activities relating to Passport's specialty network, inter-Provider communications and pharmacy authorizations. This survey is fielded to a random

sample of Providers each year. If your office is selected to participate, please take a few minutes to complete and return the survey.

Effectiveness of Quality Improvement Initiatives

Passport monitors the effectiveness of clinical and service activities through metrics selected to demonstrate clinical outcomes and service levels. The plan's performance is compared to that of available national benchmarks indicating "best practices." The evaluation includes an assessment of clinical and service improvements on an ongoing basis. Results of these measurements guide activities for the successive periods.

In addition to the methods described above, Passport also compiles complaint and appeals data as well as requests for out-of-network services to determine opportunities for service improvements

What Can Providers Do?

- Ensure patients are up to date with their annual physical exam and preventive health screenings, including related lab orders and referrals to specialists, such as ophthalmology.
- Review the HEDIS® preventive care listing of measures for each patient to determine if anything applicable to your patients' age and/or condition has been missed.
- Check that staff are properly coding all services provided.
- Be sure patients understand what *they* need to do.

Passport has additional resources to assist Providers and their patients. For access to tools that can assist, please visit the SKYGEN portal. There are a variety of resources, including HEDIS® CDT/CMS-approved diagnostic and procedural code sheets. To obtain a current list of HEDIS® and CAHPS® Star Ratings measures, contact your local Passport Quality department.

9. Risk Adjustment Management Program

What is Risk Adjustment?

CMS defines risk adjustment as a process that helps to accurately measure the health status of a plan's membership based on medical conditions and demographic information.

This process helps ensure health plans receive accurate payment for services provided to Passport Members and prepares for resources that may be needed in the future to treat Members who have chronic conditions.

Interoperability

The Provider agrees to deliver relevant clinical documents (Clinical Document Architecture (CDA) or Continuity of Care Document (CCD) format) at encounter close for Passport Members

by using one of the automated methods available and supported by the Provider's electronic medical records (EMR), including but not limited to Epic Payer Platform, Direct Protocol, Secure File Transfer Protocol (sFTP), query or Web service interfaces such as Simple Object Access Protocol (External Data Representation) or Representational State Transfer (Fast Healthcare Interoperability Resource).

The CDA or CCD document should include signed clinical note or conform with the United States Core Data for Interoperability (USCDI) common data set and Health Level 7 (HL7) Consolidated Clinical Data Architecture (CCDA) standard.

The Provider will participate in Passport's program to communicate Clinical Information using the Direct Protocol. Direct Protocol is the HIPAA-compliant mechanism for exchanging Healthcare information that is approved by the Office of the National Coordinator for Health Information Technology (ONC).

- If the Provider does not have a Direct Address, the Provider will work with its EMR vendor to set up a Direct Messaging Account, which also supports the CMS requirement of having the Provider's Digital Contact Information added in NPPES.
- If the Provider's EMR does not support the Direct Protocol, the Provider will work with Passport's established interoperability partner to get an account established.

Your Role as a Provider

As a Provider, complete and accurate documentation in a medical record is critical to a Member's quality of care. We encourage Providers to record all diagnoses to the highest specificity. This will ensure Passport receives adequate resources to provide quality programs to you and our Members.

For a complete and accurate medical record, all Provider documentation must:

- Address clinical data elements (e.g., diabetic patient needs an eye exam or multiple comorbid conditions) provided by Passport and reviewed with the Member
- Be compliant with the CMS National Correct Coding Initiative (NCCI)
- Use the correct ICD-10 code by documenting the condition to the highest level of specificity
- Only use diagnosis codes confirmed during a Provider visit with the Member. The visit may be face-to-face or telehealth, depending on state or CMS requirements.
- Contain a treatment plan and progress notes
- Contain the Member's name and date of service
- Have the Provider's signature and credentials

Contact Information

For questions about Passport's risk adjustment programs, please contact your Passport Provider Relations representative.

10. Compliance

Fraud, Waste, and Abuse

Introduction

Passport is dedicated to the detection, prevention, investigation and reporting of potential Healthcare fraud, waste, and abuse. As such, Passport's Compliance department maintains a comprehensive plan, which addresses how Passport will uphold and follow state and federal statutes and regulations pertaining to fraud, waste, and abuse. The plan also addresses fraud, waste and abuse prevention, detection, and correction along with and the education of appropriate employees, vendors, Providers, and associates doing business with Passport.

Passport's Special Investigation Unit (SIU) supports Compliance in its efforts to prevent, detect, and correct fraud, waste and abuse by conducting investigations aimed at identifying suspect activity and reporting these findings to the appropriate regulatory and/or law enforcement agency.

Mission Statement

Our mission is to pay claims correctly the first time and that mission begins with the understanding that we need to proactively detect fraud, waste, and abuse, correct it and prevent it from reoccurring. Since not all fraud, waste or abuse can be prevented, Passport employs processes that retrospectively address fraud, waste or abuse that may have already occurred. Passport strives to detect, prevent, investigate and report suspected Healthcare fraud, waste, and abuse to reduce Healthcare costs and to promote quality Healthcare.

Regulatory Requirements

Federal False Claims Act

The False Claims Act is a federal statute that covers fraud involving any federally funded contract or program. The act establishes liability for any person who knowingly presents or causes to be presented a false or fraudulent claim to the U.S. government for payment.

The term "knowing" is defined to mean that a person with respect to information:

- Has actual knowledge of falsity of information in the Claim
- Acts in deliberate ignorance of the truth or falsity of the information in a Claim
- Acts in reckless disregard of the truth or falsity of the information in a Claim

The Act does not require proof of a specific intent to defraud the U.S. government. Instead, Healthcare Providers can be prosecuted for a wide variety of conduct that leads to the submission of fraudulent claims to the government, such as knowingly making false statements, falsifying records, double billing for items or services, submitting bills for services never performed or items never furnished or otherwise causing a false Claim to be submitted.

Deficit Reduction Act (DRA)

The DRA aims to cut fraud, waste and abuse from the Medicare and Medicaid programs.

As a contractor doing business with Passport, Providers and their staff have the same obligation to report any actual or suspected violation or fraud, waste, or abuse. Entities must have written policies that inform employees, contractors, and agents of the following:

- The federal False Claims Act and state laws pertaining to submitting false Claims
- How Providers will detect and prevent fraud, waste, and abuse
- Employee protection rights as whistleblowers
- Administrative remedies for false Claims and statements

These provisions encourage employees (current or former) and others to report instances of fraud, waste, or abuse to the government. The government may then proceed to file a lawsuit against the organization/individual accused of violating the False Claims Act. The whistleblower may also file a lawsuit independently. Cases found in favor of the government will result in the whistleblower receiving a portion of the amount awarded to the government.

Whistleblower protections state that employees who have been discharged, demoted, suspended, threatened, harassed, or otherwise discriminated against due to their role in disclosing or reporting a false Claim are entitled to all relief necessary to make the employee whole including:

- Employment reinstatement at the same level of seniority
- Two (2) times the amount of back pay plus interest
- Compensation for special damages incurred by the employee because of the employer's inappropriate actions

Affected entities who fail to comply with the law will be at risk of forfeiting all payments until compliance is made. Passport will take steps to monitor Passport contracted Providers to ensure compliance with the law. Healthcare entities (e.g., providers, facilities, delegates, and/or vendors) to which Passport has paid $5 million or more in Medicaid funds during the previous federal fiscal year (October 1-September 30) will be required to submit a signed "Attestation of Compliance with the Deficit Reduction Act of 2005, Section 6032" to Passport.

Anti-Kickback Statute (42 U.S.C. § 1320a-7b(b))

Anti-kickback Statute (AKS) is a criminal law that prohibits the knowing and willful payment of "remuneration" to induce or reward patient referrals or the generation of business involving any item or service payable by the federal Healthcare programs (e.g., drugs, supplies or Healthcare services for Medicare or Medicaid patients). In some industries, it is acceptable to reward those who refer business to you. However, in the federal Healthcare programs, paying for referrals is a crime. The statute covers the payers of kickbacks-those who offer or pay remuneration- as well as the recipients of kickbacks-those who solicit or receive remuneration.

Passport conducts all business in compliance with federal and state AKS statutes and regulations and federal and state marketing regulations. Providers are prohibited from engaging in any activities covered under this statute.

AKS statutes and regulations prohibit paying or receiving anything of value to induce or reward patient referrals or the generation of business involving any item or service payable by federal and state Healthcare programs. The phrase "anything of value" can mean cash, discounts, gifts, excessive compensation, contracts not at fair market value, etc. Examples of prohibited AKS actions include a Healthcare Provider who is compensated based on patient volume or a Provider who offers remuneration to patients to influence them to use their services.

Under Passport's policies, Providers may not offer, solicit an offer, provide or receive items of value of any kind that are intended to induce referrals of federal Healthcare program business. Providers must not, directly, or indirectly, make or offer items of value to any third party for the purpose of obtaining, retaining, or directing our business. This includes giving, favors, preferential hiring, or anything of value to any government official.

Marketing Guidelines and Requirements

Providers must conduct all marketing activities in accordance with the relevant contractual requirements and marketing statutes and regulations – both state and federal.

Under Passport's policies, marketing means any communication to a beneficiary who is not enrolled with Passport that can reasonably be interpreted as intended to influence the beneficiary to enroll with Passport's Medicaid, Marketplace, or Medicare products. This also includes communications that can be interpreted to influence a beneficiary to not enroll in or to disenroll from another health plan's products.

Restricted marketing activities vary from state to state but generally relate to the types and form of communications that health plans, Providers and others can have with Members and prospective Members. Examples of such communications include those related to enrolling Members, Member outreach and other types of communications.

Stark Statute

The Physicians Self-Referral Law (Stark Law) prohibits Providers from referring patients to receive "designated health services" payable by Medicare or Medicaid from entities with which the Provider or an immediate family member has a financial relationship unless an exception applies. Financial relationships include both ownership/investment interests and compensation arrangements. The Stark law prohibits the submission or causing the submission of Claims in violation of the law's restrictions on referrals. "Designated health services" are identified in the Physician Self-Referral Law (42 U.S.C. § 1395nn).

Sarbanes-Oxley Act of 2002

The Sarbanes-Oxley Act requires certification of financial statements by both the Chief Executive Officer and the Chief Financial Officer. The Act states that a corporation must assess the effectiveness of its internal controls and report this assessment annually to the Securities and Exchange Commission.

Definitions

Fraud means an intentional deception or misrepresentation made by a person with the knowledge that the deception could result in some unauthorized benefit to themself or some other person. It includes any act that constitutes fraud under applicable federal or state law (42 CFR § 455.2).

Waste means Healthcare spending that can be eliminated without reducing the quality of care. Quality waste includes overuse, underuse, and ineffective use. Inefficiency waste includes redundancy, delays, and unnecessary process complexity. An example would be the attempt to obtain reimbursement for items or services where there was no intent to deceive or misrepresent, however the outcome resulted in poor or inefficient billing methods (e.g., coding) causing unnecessary costs to state and federal Healthcare programs.

Abuse means Provider practices that are inconsistent with sound fiscal, business, or Dental practices and result in unnecessary costs to state and federal Healthcare programs or in reimbursement for services that are not medically necessary or that fail to meet professionally recognized standards for Healthcare. It also includes recipient practices that result in unnecessary costs to state and federal Healthcare programs (42 CFR § 455.2).

Examples of Fraud, Waste, and Abuse by a Provider

The types of questionable Provider schemes investigated by Passport include, but are not limited to the following:

- A Provider knowingly and willfully referring a Member to Healthcare facilities in which or with which the Provider has a financial relationship (Stark Law).
- Altering Claims and/or Dental record documentation to get a higher level of reimbursement.
- Balance billing a Passport Member for covered services. This includes asking the Member to pay the difference between the discounted and negotiated fees and the Provider's usual and customary fees.
- Billing and providing services to Members that are not medically necessary.
- Billing for services, procedures and/or supplies that have not been rendered.
- Billing under an invalid place of service to receive or maximize reimbursement.
- Completing certificates of medical necessity for Members, not personally and professionally known by the Provider.
- Concealing a Member's misuse of a Passport Member identification card.

- Failing to report a Member's forgery or alteration of a prescription or other medical document.
- False coding to receive or maximize reimbursement.
- Inappropriate billing of modifiers to receive or maximize reimbursement.
- Inappropriately billing of a procedure that does not match the diagnosis to receive or maximize reimbursement.
- Knowingly and willfully soliciting or receiving payment of kickbacks or bribes in exchange for referring patients.
- Not following incident-to-billing guidelines to receive or maximize reimbursement.
- Overutilization
- Participating in schemes that involve collusion between a Provider and a Member that result in higher costs or charges.
- Questionable prescribing practices.
- Unbundling services to get more reimbursement, which involves separating a procedure into parts and charging for each part rather than using a single global code.
- Underutilization, which means failing to provide services that are medically necessary.
- Upcoding, which is when a Provider does not bill the correct code for the service rendered and instead uses a code for a like service that costs more.
- Using the adjustment payment process to generate fraudulent payments.

Examples of Fraud, Waste, and Abuse by a Member

The types of questionable Member schemes investigated by Passport include, but are not limited to, the following:

- Benefit sharing with persons not entitled to the Member's benefits
- Conspiracy to defraud state and federal Healthcare programs
- Doctor shopping, which occurs when a Member consults several Providers for the purpose of inappropriately obtaining services
- Falsifying documentation to get services approved
- Forgery related to Healthcare
- Prescription diversion, which occurs when a Member obtains a prescription from a Provider for a condition that they do not suffer from, and the Member sells the medication to someone else

Review of Provider Claims and Claims system

Passport Claims examiners are trained to recognize unusual billing practices, which are key in trying to identify fraud, waste, and abuse. If the Claims examiner suspects fraudulent, abusive, or wasteful billing practices, the billing practice is documented and reported to the SIU through our Compliance Alertline/reporting repository.

The Claim payment system utilizes system edits and flags to validate those elements of Claims are billed in accordance with standardized billing practices, ensure that Claims are processed accurately and ensure that payments reflect the service performed as authorized.

Passport performs auditing to ensure the accuracy of data input into the Claim system. The Claims department conducts regular audits to identify system issues or errors. If errors are identified, they are corrected, and a thorough review of system edits is conducted to detect and locate the source of the errors.

Prepayment of Fraud, Waste, and Abuse Detection Activities

Through the implementation of Claim edits, Passport's Claim payment system is designed to audit Claims concurrently to detect and prevent paying Claims that are inappropriate.

Passport has a pre-payment Claim auditing process that identifies frequent correct coding billing errors ensuring that Claims are coded appropriately according to state and federal coding guidelines. Code edit relationships and edits are based on guidelines from specific state Medicaid guidelines, federal CMS guidelines, American Dental Association (ADA) and published specialty-specific coding rules. Code edit rules are based on information received from the National Physician Fee Schedule Relative File (NPFS), the Medically Unlikely Edit (MUE) table, National Correct Coding Initiative (NCCI) files, Local Coverage Determination/National Coverage Determination (LCD/NCD) and state-specific policy manuals and guidelines as specified by a defined set of indicators in the Medicare Physician Fee Schedule Data Base (MPFSDB).

Additionally, Passport may, at the request of a state program or at its own discretion, subject a Provider to prepayment reviews whereas the Provider is required to submit supporting source documents that justify the amount charged. Where no supporting documents are provided or insufficient information is provided to substantiate a charge, the claim will be denied until such time that the Provider can provide sufficient accurate support.

Post-Payment Recovery Activities

The terms expressed in this section of this Provider Manual are incorporated into the Provider Agreement with Passport and are intended to supplement, rather than diminish, all other rights and remedies that may be available to Passport under the Provider Agreement with Passport or at law or equity.

In the event of any inconsistency between the terms expressed here and any terms expressed in the Provider Agreement with Passport, the parties agree that Passport shall in its sole discretion exercise the terms that are expressed in the Provider Agreement with Passport, the terms that are expressed here, its rights under law and equity or some combination thereof.

The Provider will provide Passport, governmental agencies and their representatives or agents, access to examine, audit and copy all records deemed by Passport, in Passport's sole discretion, necessary to determine compliance with the terms of the Provider Agreement with Passport,

including for the purpose of investigating potential fraud, waste and abuse. Documents and records must be readily accessible at the location where the Provider provides services to any Passport Members. Auditable documents and records include but are not limited to medical charts, patient charts, billing records and coordination of benefits information. Production of auditable documents and records must be provided in a timely manner, as requested by Passport and without charge to Passport. In the event Passport identifies fraud, waste or abuse, the Provider agrees to repay funds, or Passport may seek recoupment.

If a Passport auditor is denied access to the Provider's records, all the Claims for which the Provider received payment from Passport is immediately due and owing. If the Provider fails to provide all requested documentation for any claim, the entire amount of the paid Claim is immediately due and owing. Passport may offset such amounts against any amounts owed by Passport to the Provider. The Provider must comply with all requests for documentation and records timely (as reasonably requested by Passport) and without charge to Passport. Claims for which the Provider fails to furnish supporting documentation during the audit process are not reimbursable and are subject to chargeback.

The Provider acknowledges that HIPAA specifically permits a covered entity, such as the Provider, to disclose protected health information for its own payment purposes (see 45 CFR 164.502 and 45 CFR 164.501). The Provider further acknowledges that to receive payment from Passport, the Provider is required to allow Passport to conduct audits of its pertinent records to verify the services performed and the payment claimed and that such audits are permitted as a payment activity of the Provider under HIPAA and other applicable privacy laws.

Claim Auditing

Passport shall use established industry Claim adjudication and/or clinical practices, state and federal guidelines, and/or Passport's policies and data to determine the appropriateness of the billing, coding, and payment.

The Provider acknowledges Passport's right to conduct pre- and post-payment billing audits. The Provider shall cooperate with Passport's SIU and audits of Claims and payments by providing access at reasonable times to requested Claims information, the Provider's charging policies and other related data as deemed relevant to support the transactions billed. Additionally, Providers are required, by contract and in accordance with the Provider Manual to submit all supporting medical records/documentation as requested. Failure to do so in a timely manner may result in an audit failure and/or denial resulting in an overpayment.

In reviewing medical records for a procedure, Passport reserves the right and where unprohibited by regulation, to select a statistically valid random sample or smaller subset of the statistically valid random sample. This gives an estimate of the proportion of Claims that Passport paid in error. The estimated proportion or error rate may be extrapolated across all Claims to determine the amount of overpayment.

Provider audits may be telephonic, an on-site visit, internal Claims review, client-directed/regulatory investigation and/or compliance reviews and may be vendor-assisted. Passport asks that you provide Passport or Passport's designee, during normal business hours, access to examine, audit, scan and copy all records necessary to determine compliance and accuracy of billing.

If Passport's SIU suspects that there is fraudulent or abusive activity, Passport may conduct an on-site audit without notice. Should you refuse to allow access to your facilities, Passport reserves the right to recover the full amount paid or due to you.

Provider Education

When Passport identifies, through an audit or other means, a situation with a Provider (e.g., coding, billing) that is either inappropriate or deficient, Passport may determine that a Provider education visit is appropriate.

Passport will notify the Provider of the deficiency and will take steps to educate the Provider, which may include the Provider submitting a CAP to Passport addressing the issues identified and how it will cure these issues moving forward.

Reporting Fraud, Waste, and Abuse

Suspected cases of fraud, waste or abuse must be reported to Passport by contacting the Passport Alertline. The Passport Alertline is an external telephone and web-based reporting system hosted by NAVEX Global, a leading provider of compliance and ethics hotline services. The Passport Alertline telephone and web-based reporting is available 24 hours a day, 7 days a week, 365 days a year. When a report is made, callers can choose to remain confidential or anonymous. When calling the Passport Alertline, a trained professional at NAVEX Global will note the caller's concerns and provide them to the Passport Compliance department for follow-up. When electing to use the web-based reporting process, a series of questions will be asked concluding with the submission of the report. Reports to the Passport Alertline can be made from anywhere within the United States with telephone or internet access.

The Passport Alertline can be reached at (866) 606-3889 or you may use the service's website to make a report at any time at MolinaHealthcare.Alertline.com.

Fraud, waste, or abuse cases may also be reported to Passport's Compliance department anonymously without fear of retaliation.

Confidential Compliance Officer
Passport by Molina Healthcare
2028 W. Broadway
Louisville, KY 40203
Phone: (866) 606-3889
Website: MolinaHealthcare.alertline.com

The following information should be included when reporting:

- Nature of complaint
- The names of individuals and/or entity involved in suspected fraud and/or abuse including address, phone number, Passport Member ID number and any other identifying information

HIPAA Requirements and Information

Passport's Commitment to Patient Privacy

Protecting the privacy of Members' personal health information is a core responsibility that Passport takes very seriously. Passport is committed to complying with all federal and state laws regarding the privacy and security of Member's protected health information (PHI).

Provider Responsibilities

Passport expects that its contracted Providers will respect the privacy of Passport Members (including Passport Members who are not patients of the Provider) and comply with all applicable laws and regulations regarding the privacy of patient and Member PHI. Passport provides its Members with a privacy notice upon their enrollment in our health plan. The privacy notice explains how Passport uses and discloses their PHI and includes a summary of how Passport safeguards their PHI.

Telehealth/telemedicine Providers: telehealth transmissions are subject to HIPAA-related requirements outlined under state and federal law, including:

- 42 C.F.R. Part 2 regulations
- Health Information Technology for Economic and Clinical Health Act, (HITECH Act)

Applicable Laws

Providers must understand all state and federal Healthcare privacy laws applicable to their practice and organization. Currently, there is no comprehensive regulatory framework that protects all health information in the United States; instead, there is a patchwork of laws that Providers must comply with. In general, most Healthcare Providers are subject to various laws and regulations pertaining to the privacy of health information, including, without limitation, the following:

1. **Federal laws and regulations**
    - HIPAA
    - HITECH
    - 42 C.F.R. Part 2
    - Medicare and Medicaid laws
    - The Affordable Care Act

2. State medical privacy laws and regulations.

Providers should be aware that HIPAA provides a floor for patient privacy but that state laws should be followed in certain situations, especially if the state law is more stringent than HIPAA. Providers should consult with their own legal counsel to address their specific situation.

Artificial Intelligence

The Provider shall comply with all applicable state, and federal laws and regulations related to artificial intelligence and the use of artificial intelligence tools (AI). Artificial Intelligence or AI means a machine-based system that can, with respect to a given set of human-defined objectives, input, or prompt, as applicable, make predictions, recommendations, data sets, work product (whether eligible for copyright protection), or decisions influencing physical or virtual environments. The Provider is prohibited from using AI for any functions that result in a denial, delay, reduction, or modification of covered services to Passport Members including, but not limited to utilization management, prior authorizations, complaints, appeals and grievances, and quality of care services, without review of the denial, delay, reduction, or modification by a qualified clinician.

Notwithstanding the foregoing, the Provider shall give advance written notice to your Passport Contract Manager (for any AI used by the Provider that may impact the provision of covered services to Passport Members) that describes (i) Providers' use of the AI tool(s) and (ii) how the Provider oversees, monitors and evaluates the performance and legal compliance of such AI tool(s). If the use of AI is approved by Passport, the Provider further agrees to (i) allow Passport to audit Providers' AI use, as requested by Passport from time to time, and (ii) to cooperate with Password regarding any regulatory inquiries and investigations related to Providers' AI use related to the provision of covered services to Passport Members.

If you have additional questions, please contact your Passport Contract Manager.

Uses and Disclosures of PHI

Member and patient PHI should only be used or disclosed as permitted or required by applicable law. Under HIPAA, a Provider may use and disclose PHI for their own treatment, payment, and Healthcare operations activities (TPO) without the consent or authorization of the patient who is the subject of the PHI. Uses and disclosures for TPO apply not only to the Provider's own TPO activities, but also for the TPO of another covered entity[1]. Disclosure of PHI by one covered entity to another covered entity or Healthcare Provider, for the recipient's TPO is specifically permitted under HIPAA in the following situations:

1. A covered entity may disclose PHI to another covered entity or a Healthcare Provider for the payment activities of the recipient. Please note that "payment" is a defined term

[1] See Sections 164.506(c) (2) & (3) of the HIPAA Privacy Rule.

under the HIPAA Privacy Rule that includes, without limitation, utilization review activities, such as preauthorization of services, concurrent review, and retrospective review of services[2].

2. A covered entity may disclose PHI to another covered entity for the Healthcare operations activities of the covered entity that receives the PHI, if each covered entity either has or had a relationship with the individual who is the subject of the PHI being requested, the PHI pertains to such relationship, and the disclosure is for the following Healthcare operations activities:
    - Quality improvement
    - Disease management
    - Case management and care coordination
    - Training programs
    - Accreditation, licensing, and credentialing

Importantly, this allows Providers to share PHI with Passport for our Healthcare operations activities, such as HEDIS® and quality improvement.

Confidentiality of Substance Abuse Disorder Patient Records

Federal confidentiality of substance use disorder patient records regulations apply to any entity or individual providing federally assisted alcohol or drug abuse prevention treatment. Records of the identity, diagnosis, prognosis, or treatment of any patient which are maintained in connection with substance use disorder treatment or programs are confidential and may be disclosed only as permitted by 42 CFR Part 2. Although HIPAA protects substance use disorder information, the federal confidentiality of substance use disorder patient records regulations are more restrictive than HIPAA and they do not allow disclosure without the Member's written consent except as set forth in 42 CFR Part 2.

Inadvertent Disclosures of PHI

Passport may, on occasion, inadvertently misdirect or disclose PHI pertaining to Passport Member(s) who are not the patients of the Provider. In such cases, the Provider shall return or securely destroy the PHI of the affected Passport Members to protect their privacy. The Provider agrees to not further use or disclose such PHI and further agrees to provide an attestation of return, destruction, and non-disclosure of any such misdirected PHI upon the reasonable request of Passport.

[2] See the definition of Payment, Section 164.501 of the HIPAA Privacy Rule

Written Authorizations

Uses and disclosures of PHI that are not permitted or required under applicable law require the valid written authorization of the patient. Authorizations should meet the requirements of HIPAA and applicable state law.

Patient Rights

Patients are afforded various rights under HIPAA. Passport Providers must allow patients to exercise any of the below-listed rights that apply to the Provider's practice:

1. Notice of privacy practices
2. Providers that are covered under HIPAA and that have a direct treatment relationship with the patient should provide patients with a notice of privacy practices that explains the patient's privacy rights and the process the patient should follow to exercise those rights. The Provider should obtain a written acknowledgment that the patient received the notice of privacy practices
3. Requests for restrictions on use and disclosures of PHI
4. Patients may request that a Healthcare Provider restrict its uses and disclosures of PHI
5. The Provider is not required to agree to any such request for restrictions
6. Requests for confidential communications
7. Patients may request that a Healthcare Provider communicate PHI by alternative means or at alternative locations. Providers must accommodate reasonable requests from the patient
8. Requests for Patient Access to PHI
9. Patients have a right to access their own PHI within a Provider's designated record set
10. Personal representatives of patients have the right to access the PHI of the subject patient. The designated record set of a Provider includes the patient's medical record, as well as billing and other records used to make decisions about the Member's care or payment for care
11. Request to amend PHI
12. Patients have a right to request that the Provider amend information in their designated record set
13. Request accounting of PHI disclosures
14. Patients may request an accounting of disclosures of PHI made by the Provider during the preceding six (6) year period. The list of disclosures does not need to include disclosures made for treatment, payment, or Healthcare operations

HIPAA Security

Providers must implement and maintain reasonable and appropriate safeguards to protect the confidentiality, availability and integrity of Passport Member and patient PHI. As more Providers implement electronic health records, Providers need to ensure that they have implemented and maintain appropriate cybersecurity measures. Providers should recognize that identity theft - both financial and medical - is a rapidly growing problem and that their

patients trust their Healthcare Providers to keep their most sensitive information private and confidential.

Medical identity theft is an emerging threat in the Healthcare industry. Medical identity theft occurs when someone uses a person's name and sometimes other parts of their identity - such as health insurance information - without the person's knowledge or consent to obtain Healthcare services or goods. Medical identity theft frequently results in erroneous entries being put into existing medical records. Providers should be aware of this growing problem and report any suspected fraud to Passport.

HIPAA Transactions and Code Sets

Passport strongly supports the use of electronic transactions to streamline Healthcare administrative activities. Passport Providers are encouraged to submit Claims and other transactions to Passport using electronic formats. Certain electronic transactions in Healthcare are subject to HIPAA's Transactions and Code Sets Rule including, but not limited to, the following:

- Claims and Encounters
- Member eligibility status inquiries and responses
- Claims status inquiries and responses
- Authorization requests and responses
- Remittance advice

Passport is committed to complying with all HIPAA Transaction and Code Sets standard requirements. Providers should refer to Passport's website at MolinaHealthcare.com for additional information regarding HIPAA standard transactions.

1. Click on the area titled "Healthcare Professionals"
2. Click the tab titled "HIPAA"
3. Click on the tab titled "HIPAA Transactions" or "HIPAA Code Sets"

Code Sets

HIPAA regulations require that only approved code sets may be used in standard electronic transactions.

National Provider Identifier (NPI)

Providers must comply with the NPI rule promulgated under HIPAA. The Provider must obtain an NPI from NPPES for itself or for any subparts of the Provider. The Provider must report its NPI and any subparts to Passport and to any other entity that requires it. Any changes in its NPI or subparts information must be reported to NPPES within 30 days and should also be reported to Passport within 30 days of the change. Providers must use their NPI to identify it on all electronic transactions required under HIPAA and on all Claims and Encounters submitted to Passport.

Additional Requirements for Delegated Providers

Providers that are delegated for Claims and utilization management activities are the "business associates" of Passport. Under HIPAA, Passport must obtain contractual assurances from all business associates that will safeguard Member PHI. Delegated Providers must agree to various contractual provisions required under HIPAA's privacy and security rules.

Reimbursement for Copies of PHI

Passport does not reimburse Providers for copies of PHI related to our Members. These requests may include, although they are not limited to, the following purposes:

- Utilization management
- Care coordination and/or complex medical care management services
- Claims review
- Resolution of an appeal and/or grievance
- Anti-fraud program review
- Quality of care issues
- Regulatory audits
- Risk adjustment
- Treatment, payment, and/or operation purposes
- Collection of HEDIS® medical records

Information Security and Cybersecurity

NOTE: This section (Information Security and Cybersecurity) is only applicable to Providers who have been delegated by Passport to perform a health plan function(s) and in connection with such delegated functions.

1. Definitions:
    - "Passport Information" means any information: (i) provided by Passport to Provider; (ii) accessed by Provider or available to Provider on Passport's Information Systems; or (iii) any information with respect to Passport or any of its consumers developed by Provider or other third parties in Provider's possession, including without limitation any Passport Nonpublic Information.
    - "Cybersecurity Event" means any actual or reasonably suspected contamination, penetration, unauthorized access or acquisition or other breach of confidentiality, data integrity or security compromise of a network or server resulting in the known or reasonably suspected accidental, unauthorized, or unlawful destruction, loss, alteration, use, disclosure of or access to Passport Information. For clarity, a Breach, or Security Incident as these terms are defined under HIPAA constitute a Cybersecurity Event for the purpose of this section. Unsuccessful security incidents, which are activities such as pings and other broadcast attacks on Provider's firewall, port scans, unsuccessful log-on attempts, denials of service and any combination of

the above, do not constitute a Cybersecurity Event under this definition so long as no such incident results in or is reasonably suspected to have resulted in unauthorized access, use, acquisition or disclosure of Passport Information or sustained interruption of service obligations to Passport.

- "HIPAA" means the Health Insurance Portability and Accountability Act, as may be amended from time to time.
- "HITECH" means the Health Information Technology for Economic and Clinical Health Act, as may be amended from time to time.

2. "Industry Standards" mean as applicable, codes, guidance (from regulatory and advisory bodies, whether mandatory or not), international and national standards, relating to security of network and information systems and security breach and incident reporting requirements, all as amended or updated from time to time and including but not limited to the current standards and benchmarks set forth and maintained by the following, in accordance with the latest revisions and/or amendments:
    i. HIPAA and HITECH
    ii. HITRUST Common Security Framework
    iii. Center for Internet Security
    iv. National Institute for Standards and Technology ("NIST") Special Publications 800.53 Rev.5 and 800.171 Rev. 1 or as currently revised
    v. Federal Information Security Management Act ("FISMA")
    vi. ISO/ IEC 27001
    vii. Federal Risk and Authorization Management Program ("FedRamp")
    viii. NIST Special Publication 800-34 Revision 1 – "Contingency Planning Guide for Federal Information Systems."
    ix. International Organization for Standardization (ISO) 22301 – "Societal security – Business continuity management systems – Requirements."
3. "Information Systems" means all computer hardware, databases and data storage systems, computer, data, database, and communications networks (other than the Internet), cloud platform, architecture interfaces and firewalls (whether for data, voice, video or other media access, transmission, or reception) and other apparatus used to create, store, transmit, exchange or receive information in any form.
4. "Multi-Factor Authentication" means authentication through verification of at least two of the following types of authentication factors: (1) knowledge factors, such as a password; (2) possession factors, such as a token or text message on a mobile phone; (3) inherence factors, such as a biometric characteristic; or (4) any other industry standard and commercially accepted authentication factors.
5. "Nonpublic Information" includes:
    i. Passport's proprietary and/or confidential information.
    ii. Personally Identifiable Information as defined under applicable state data security laws, including, without, limitation, "nonpublic personal information," "personal

data," "personally identifiable information," "personal information" or any other similar term as defined pursuant to any applicable law; and

iii. Protected Health Information as defined under HIPAA and HITECH.

6. Information Security and Cybersecurity Measures. Provider shall implement and always maintain appropriate administrative, technical, and physical measures to protect and secure the Information Systems, as well as Nonpublic Information stored thereon and Passport Information that are accessible to or held by Provider. Such measures shall conform to generally recognized industry standards and best practices and shall comply with applicable privacy and data security laws, including implementing and maintaining administrative, technical, and physical safeguards pursuant to HIPAA, HITECH, and other applicable U.S. federal, state, and local laws.

7. Policies, Procedures and Practices. Provider must have policies, procedures and practices that address its information security and cybersecurity measures, safeguards, and standards, including as applicable, a written information security program, which Passport shall be permitted to audit via written request, and which shall include at least the following:
    - Access Controls. Access controls, including Multi-Factor Authentication, to limit access to the Information Systems and Passport Information accessible to or held by Provider.
    - Encryption. Use of encryption to protect Passport Information, in transit and at rest, accessible to or held by Provider.
    - Security. Safeguarding the security of the Information Systems and Passport Information accessible to or held by Provider, which shall include hardware and software protections such as network firewall provisioning, intrusion and threat detection controls designed to protect against malicious code and/or activity, regular (three or more annually) third party vulnerability assessments, physical security controls and personnel training programs that include phishing recognition and proper data management hygiene.
    - Software Maintenance. Software maintenance, support, updates, upgrades, third party software components and bug fixes such that the software is and remains secure from vulnerabilities in accordance with the applicable Industry Standards.
8. Technical Standards. Provider shall comply with the following requirements and technical standards related to network and data security:
    a. Network Security. Network security shall conform to generally recognized industry standards and best practices. Generally recognized industry standards include, but are not limited to, the applicable Industry Standards.
    b. Cloud Services Security: If Provider employs cloud technologies, including infrastructure as a service (IaaS), software as a service (SaaS) or platform as a service (PaaS), for any services, Provider shall adopt a "zero-trust architecture" satisfying the requirements described in NIST 800-207 (or any successor cybersecurity framework thereof).

c. Data Storage. Provider agrees that all Passport Information will be stored, processed, and maintained solely on designated target servers or cloud resources. No Passport Information at any time will be processed on or transferred to any portable or laptop computing device or any portable storage medium, unless that device or storage medium is in use as part of the Provider's designated backup and recovery processes and is encrypted in accordance with the requirements set forth herein.
d. Data Encryption. Provider agrees to store all Passport Information as part of its designated backup and recovery processes in encrypted form, using a commercially supported encryption solution. Provider further agrees that all Passport Information stored on any portable or laptop computing device or any portable storage medium be likewise encrypted. Encryption solutions will be deployed with no less than a 128-bit key for symmetric encryption, a 1024 (or larger) bit key length for asymmetric encryption and the Federal Information Processing Standard Publication 140-2 ("FIPS PUB 140-2").
e. Data Transmission. Provider agrees that all electronic transmission or exchange of system and application data with Passport and/or any other parties expressly designated by Passport shall take place via secure means (using HTTPS or SFTP or equivalent) and solely in accordance with FIPS PUB 140-2 and the Data Re-Use requirements set forth herein.
f. Data Re-Use. Provider agrees that all Passport Information exchanged shall be used expressly and solely for the purposes enumerated in the Provider Agreement with Passport and this section. Data shall not be distributed, repurposed, or shared across other applications, environments, or business units of Provider. Provider further agrees that no Passport Information or data of any kind shall be transmitted, exchanged, or otherwise passed to other affiliates, contractors or interested parties, except on a case-by-case basis as specifically agreed to in advance and in writing by Passport.

9. Business Continuity ("BC") and Disaster Recovery ("DR"). Provider shall have documented procedures in place to ensure continuity of Provider's business operations, including disaster recovery, in the event of an incident that has the potential to impact, degrade or disrupt Provider's delivery of services to Passport.

10. Resilience Questionnaire. Provider shall complete a questionnaire provided by Passport to establish Provider's resilience capabilities.

11. BC/DR Plan.
    a. Provider's procedures addressing continuity of business operations, including disaster recovery, shall be collected and/or summarized in a documented BC and DR plan or plans in written format ("BC/DR Plan"). The BC/DR Plan shall identify the service level agreement(s) established between Provider and Passport. The BC/DR Plan shall include the following:
        i. Notification, escalation, and declaration procedures.
        ii. Roles, responsibilities and contact lists.
        iii. All Information Systems that support services provided to Passport.

iv. Detailed recovery procedures in the event of the loss of people, processes, technology and/or third parties or any combination thereof providing services to Passport.
v. Recovery procedures in connection with a Cybersecurity Event, including ransomware.
vi. Detailed list of resources to recover services to Passport including but not limited to applications, systems, vital records, locations, personnel, vendors, and other dependencies.
vii. Detailed procedures to restore services from a Cybersecurity Event including ransomware.

12. Documented risk assessment which shall address and evaluate the probability and impact of risks to the organization and services provided to Passport. Such risk assessment shall evaluate natural, man-made, political and cybersecurity incidents.
    a. To the extent that Passport Information is held by Provider, Provider shall maintain backups of such Passport Information that are adequately protected from unauthorized alterations or destruction consistent with applicable Industry Standards.
    b. Provider shall develop information technology disaster recovery or systems contingency plans consistent with applicable Industry Standards and in accordance with all applicable laws.
13. Notification. Provider shall notify Passport's Chief Information Security Officer by telephone and email (provided herein) as promptly as possible, but not to exceed 24 hours, of either of the following:
    a. Provider's discovery of any potentially disruptive incident that may impact or interfere with the delivery of services to Passport that detrimentally affects Provider's Information Systems or Passport's Information.
    b. Provider's activation of business continuity plans. Provider shall provide Passport with regular updates by telephone or email (provided herein) on the situation and actions taken to resolve the issue, until normal services have been resumed.
14. BC and DR Testing. For services provided to Passport, Provider shall exercise its BC/DR Plan at least once each calendar year. Provider shall exercise its cybersecurity recovery procedures at least once each calendar year. At the conclusion of the exercise, Provider shall provide Passport a written report in electronic format upon request. At a minimum, the written report shall include the date of the test(s), objectives, participants, a description of activities performed, results of the activities, corrective actions identified and modifications to plans based on results of the exercise(s).
15. Cybersecurity Events. Provider agrees to comply with all applicable data protection and privacy laws and regulations. Provider will implement best practices for incident management to identify, contain, respond to, and resolve Cybersecurity Events.

    In the event of a Cybersecurity Event that threatens or affects Passport's Information Systems (in connection with Provider having access to such Information Systems); Provider's Information Systems; or Passport Information accessible to or held by Provider, Provider shall notify Passport's Chief Information Security Officer of such

event by telephone and email as provided below (with follow-up notice by mail) as promptly as possible, but in no event later than 24 hours from Provider's discovery of the Cybersecurity Event.

If Provider makes a ransom or extortion payment in connection with a Cybersecurity Event that involves or may involve Passport Information, Provider shall notify Passport's Chief Information Security Officer (by telephone and email, with follow-up notice by mail) within 24 hours following such payment.

Within 15 days of such a ransom payment that involves or may involve Passport Information, Provider shall provide a written description of the reasons for which the payment was made, a description of alternatives to payment considered, a description of due diligence undertaken to find alternatives to payment and evidence of all due diligence and sanctions checks performed in compliance with applicable rules and regulations, including those of the Office of Foreign Assets Control.

16. Notification to Passport's Chief Information Security Officer shall be provided to:
    - Passport Chief Information Security Officer
    - Telephone: (844) 821-1942
    - Email: CyberIncidentReporting@Molinahealthcare.com
    - Passport Chief Information Security Officer
      Passport by Molina Healthcare
      200 Oceangate Blvd., Suite 100
      Long Beach, CA 90802
17. In the event of a Cybersecurity Event, Provider will, at Passport's request, (i) fully cooperate with any investigation concerning the Cybersecurity Event by Passport, (ii) fully cooperate with Passport to comply with applicable law concerning the Cybersecurity Event, including any notification to consumers and (iii) be liable for any expenses associated with the Cybersecurity Event including without limitation: (a) the cost of any required legal compliance (e.g., notices required by applicable law) and (b) the cost of providing two (2) years of credit monitoring services or other assistance to affected consumers. In no event will Provider serve any notice of or otherwise publicize a Cybersecurity Event involving Passport Information without the prior written consent of Passport.
18. Following notification of a Cybersecurity Event, Provider must promptly provide Passport any documentation requested by Passport to complete an investigation, or, upon request by Passport, complete an investigation pursuant to the following requirements:
    a. make a determination as to whether a Cybersecurity Event occurred.
    b. assess the nature and scope of the Cybersecurity Event.
    c. identify Passport's Information that may have been involved in the Cybersecurity Event; and

d. perform or oversee reasonable measures to restore the security of the Information Systems compromised in the Cybersecurity Event to prevent further unauthorized acquisition, release, or use of Passport Information.

19. Provider must provide Passport the following required information regarding a Cybersecurity Event in electronic form. Provider shall have a continuing obligation to update and supplement the initial and subsequent notifications to Passport concerning the Cybersecurity Event. The information provided to Passport must include at least the following, to the extent known:

    a. the date of the Cybersecurity Event.
    b. a description of how the information was exposed, lost, stolen, or breached.
    c. how the Cybersecurity Event was discovered.
    d. whether any lost, stolen, or breached information has been recovered and if so, how this was done.
    e. the identity of the source of the Cybersecurity Event.
    f. whether Provider has filed a police report or has notified any regulatory, governmental or law enforcement agencies and, if so, when such notification was provided.
    g. a description of the specific types of information accessed or acquired without authorization, which means data elements including, for example, types of medical information, types of financial information or types of information allowing identification of the consumer.
    h. the period during which the Information System was compromised by the Cybersecurity Event.
    i. the number of total consumers in each state affected by the Cybersecurity Event.
    j. the results of any internal review identifying a lapse in either automated controls or internal procedures or confirming that all automated controls or internal procedures were followed.
    k. a description of efforts being undertaken to remediate the situation which permitted the Cybersecurity Event to occur.
    l. a copy of Provider's privacy policy and a statement outlining the steps Provider will take to investigate and if requested by Passport, the steps that Provider will take to notify consumers affected by the Cybersecurity Event; and
    m. the name of a contact person who is familiar with the Cybersecurity Event and authorized to act on behalf of Provider.

    n. Provider shall maintain records concerning all Cybersecurity Events for a period of at least five (5) years from the date of the Cybersecurity Event or such longer period as required by applicable laws and produce those records upon Passport's request.

20. Right to Conduct Assessments; Provider Warranty. Provider agrees to fully cooperate with any security risk assessments performed by Passport and/or any designated representative or vendor of Passport. Provider agrees to promptly provide accurate and

complete information with respect to such security risk assessments. If Passport performs a due diligence/security risk assessment of Provider, Provider (i) warrants that the services provided pursuant to the Provider Agreement with Passport will be in compliance with generally recognized industry standards and as provided in Provider's response to Passport's due diligence/security risk assessment questionnaire; (ii) agrees to inform Passport promptly of any material variation in operations from what was provided in Provider's response to Passport's due diligence/security risk assessment; and (iii) agrees that any material deficiency in operations from those as described in the Provider's response to Passport's due diligence/security risk assessment questionnaire may be deemed a material breach of the Provider Agreement with Passport.

21. Other Provisions. Provider acknowledges that there may be other information security and data protection requirements applicable to Provider in the performance of services which may be addressed in an agreement between Passport and Provider but are not contained in this section.
22. Conflicting Provisions. In the event of any conflict between the provisions of this section and any other agreement between Passport and Provider, the stricter of the conflicting provisions will control.

11. Claims and Compensation

Payer ID	**SKYGN WITHOUT THE "E"**
SKYGEN portal	SKYGEN
Clean claim Timely filling	**365 calendar days from the date of service**

Electronic Claim Submission

Passport strongly encourages participating Providers to submit Claims electronically, including secondary Claims. Electronic Claim submission provides significant benefits to the Provider including:

- Helps to reduce operation costs associated with Paper Claims (printing, postage, etc.)
- Increases accuracy of data and efficient information delivery
- Reduces Claim delays since errors can be corrected and resubmitted electronically
- Eliminates mailing time and Claims reach Passport faster

Passport offers the following electronic Claim submission options:

- Submit Claims directly to Passport via the SKYGEN portal
- Submit Claims to Passport via your regular EDI clearinghouse

SKYGEN Dental Hub

The SKYGEN portal is a no-cost online platform that offers several Claims processing features:

- Submit Professional ADA Claims with attached files
- Correct/void Claims

- Add attachments to previously submitted Claims
- Check Claim status
- View ERA and EOP
- Create and manage Claim templates
- Create and submit a Claim appeal with attached files

Clearinghouse

Providers can submit Claims to SKYGEN via a clearinghouse.

SKYGEN accepts EDI transactions for Claims via the 837P for Professional and 837I for institutional. It is important to track your electronic transmissions using your acknowledgement reports. The reports assure Claims are received for processing in a timely manner.

When your Claims are filed via a clearinghouse:

- You should receive a 999 acknowledgment from your clearinghouse
- You should also receive 277CA response file with initial status of the Claims from your clearinghouse
- You should refer to the Passport Companion Guide for information on the response format and messages
- You should contact your local clearinghouse representative if you experience any problems with your transmission

EDI Claim Submission Issues

Providers who are experiencing EDI submission issues should work with their clearinghouse to resolve this issue. If the Provider's clearinghouse is unable to resolve, the Provider should contact their Passport Provider Relations representative for additional support.

Timely Claim Filing

Providers shall promptly submit to Passport Claims for covered services rendered to Members. All Claims shall be submitted in a form acceptable to and approved by Passport and shall include all medical records pertaining to the Claim if requested by Passport or otherwise required by Passport's policies and procedures. Claims must be submitted by the Provider to Passport within 365 calendar days after the discharge for inpatient services or the date of service for outpatient services. If Passport is not the primary payer under the coordination of benefits or third-party liability, the Provider must submit Claims to Passport within 365 calendar days after final determination by the primary payer. Except as otherwise provided by law or provided by government program requirements, any Claims that are not submitted to Passport within these timelines shall not be eligible for payment and the Provider hereby waives any right to payment.

Claim Submission

Participating Providers are required to submit Claims to Passport with appropriate documentation. Providers must follow the appropriate state and CMS Provider billing guidelines as well as any criteria explicitly required in the Dental Provider Manual and any criteria explicitly required in the clinical guidelines. Providers must utilize electronic billing through a clearinghouse or the SKYGEN portal whenever possible and use current HIPAA-compliant American National Standards Institute (ANSI) X12N format (e.g., 837I for institutional Claims, 837P for professional Claims and 837D for dental Claims).

National Provider Identifier (NPI)

A valid NPI is required on all Claim submissions. Providers must report any changes in their NPI or subparts to Passport as soon as possible, not to exceed 30 calendar days from the change. Passport support the CMS recommendations around NPPES data verification and encourages our Provider network to verify Provider data via nppes.cms.hhs.gov. Passport may validate the NPI submitted in a Claim transaction is a valid NPI and is recognized as part of the NPPES data.

Required Elements

Electronic submitters should use the Implementation Guide and Passport Companion Guide for format and code set information when submitting or receiving files directly with Passport. In addition to the Implementation Guide and Companion Guide, electronic submitters should use the appropriate state-specific Companion Guides and Provider Manuals. These documents are subject to change as new information is available. Please check the Passport website at MolinaHealthcare.com under EDI>Companion Guides for regularly updated information regarding Passport's companion guide requirements. Be sure to choose the appropriate state from the drop-down list on the top of the page. In addition to the Passport Companion Guide, it is also necessary to use the state health plan-specific companion guides, which are also available on our Passport website for your convenience (remember to choose the appropriate state from the drop-down list).

Electronic Claim submissions will adhere to specifications for submitting medical Claim data in standardized Accredited Standards Committee (ASC) X12N 837 formats. Electronic Claims are validated for compliance with Strategic National Implementation Process (SNIP) levels 1-5.

The following information must be included on every Claim, whether electronic or paper:

- Member name, date of birth and Passport Member ID number
- Member's gender
- Member's address
- Date(s) of service
- Valid International Classification of Diseases diagnosis and procedure codes (if required)
- Valid CDT for services or items provided, if applicable
- Valid Diagnosis Pointers
- Total billed charges
- Place and type of service code

- Days or units as applicable (anesthesia Claims require minutes)
- Provider tax identification number (TIN)
- 10-digit National Provider Identifier (NPI)
- Rendering Provider information when different than billing
- Billing/Pay-to Provider name and billing address
- Place of service and type (for facilities)
- Disclosure of any other health benefit plans
- National Drug Code (NDC), NDC Units, Units of Measure and Days or Units for medical injectables
- E-signature
- Service facility location information
- Any other state-required data

Provider and Member data will be verified for accuracy and active status. Be sure to validate this data in advance of Claim submission. This validation will apply to all Provider data submitted and applies to atypical and out-of-state Providers.

Inaccurate, incomplete, or untimely submissions and re-submissions may result in denial of the Claim.

EDI (Clearinghouse) Submission

Corrected Claim information submitted via EDI submission are required to follow electronic Claim standardized ASC X12N 837 formats. Electronic Claims are validated for compliance with SNIP levels 1-5. The 837 Claim format allows you to submit changes to Claims that were not included on the original adjudication.

The 837 Implementation Guides refer to the National Uniform Billing Data Element Specifications Loop 2300 CLM05-3 for explanation and usage. In the 837 formats, the codes are called “Claim frequency codes.” Using the appropriate code, you can indicate that the Claim is an adjustment of a previously submitted finalized Claim. Use the below frequency codes for Claims that were previously adjudicated.

Claim frequency code	Description	Action
7	Use to replace an entire Claim.	Passport will adjust the original Claim. The corrections submitted represent a complete replacement of the previously processed Claim.
8	Use to eliminate a previously submitted Claim.	Passport will void the original Claim from records based on request.

When submitting Claims noted with Claim frequency code 7 or 8, the original Claim number must be submitted in Loop 2300 REF02 – Payer Claim Control Number with qualifier F8 in

REF01. The original Claim number can be obtained from the 835 ERA. Without the original Claim number, adjustment requests will generate a compliance error, and the Claim will reject.

Claim corrections submitted without the appropriate frequency code will deny as a duplicate and the original Claim number will not be adjusted.

Paper Claim Submission

Participating Providers should submit Claims electronically. If electronic Claim submission is not possible, please submit paper Claims to the following address:

Passport by Molina Healthcare
PO Box 2136
Milwaukee WI 53201

When submitting paper Claims:

- Paper Claim submissions are not considered to be "accepted" until received at the appropriate Claims PO Box; Claims received outside of the designated PO Box will be returned for appropriate submission.
- Paper Claims are required to be submitted on original ADA claim forms
- Paper Claims not submitted on the required forms will be rejected. This includes black and white forms, copied forms and any altering to include Claims with handwriting.
- Claims must be typed with either 10 or 12-point Times New Roman font, using black ink.
    - Link to paper Claims submission guidance: ADA DENTAL CLAIM FORM.

Corrected Claim Process

Providers can submit a corrected claim if the original claim or service was paid incorrectly. Providers should submit a new claim for services that were denied or not previously submitted.

Providers may correct any necessary field of the ADA claim forms.

Passport strongly encourages participating Providers to submit Corrected Claims electronically via EDI or the SKYGEN portal.

All corrected Claims:

- Must be free of handwritten or stamped verbiage (paper Claims).
- Paper Claims are required to be submitted on original ADA claim forms
- Original Claim number and the requested action must be documented in box 35 of the ADA claim form

Corrected Claims must be sent within 365 calendar days of the date of service.

Corrected Claim submission options:

- Submit Corrected Claims directly to Passport via the SKYGEN portal

- Submit corrected Claims to Passport via your regular EDI clearinghouse

Coordination of Benefits (COB) and Third-party Liability (TPL)

Third-party liability refers to any other health insurance plan or carrier (e.g., individual, group, employer-related, self-insured, self-funded or commercial carrier, automobile insurance and worker's compensation) or program that is or may be liable to pay all or part of the Healthcare expenses of the Member.

Medicaid is always the payer of last resort and Providers shall make reasonable efforts to determine the legal liability of third parties to pay for services furnished to Passport Members. If third-party liability can be established, Providers must bill the primary payer, enter the primary payment on each billing line and submit the primary explanation of benefits (EOB) to Passport for secondary Claim processing. If coordination of benefits occurs, the Provider shall be reimbursed based on the state regulatory COB methodology. Primary carrier payment information is required with the Claim submission. Providers can submit Claims with attachments, including EOB and other required documents. Passport will pay Claims for prenatal care and EPSDT and then seek reimbursement from third parties. If services and payment have been rendered prior to establishing third-party liability, an overpayment notification letter will be sent to the Provider requesting a refund including third-party policy information required for billing.

Subrogation – Passport retains the right to recover benefits paid for a Member's Healthcare services when a third party is responsible for the Member's injury or illness to the extent permitted under state and federal law and the Member's benefit plan. If third-party liability is suspected or known, please refer pertinent case information to Passport's vendor at KY – Conduent: tplefaxes@conduent.com.

Passport Coding and Payment Policies

Frequently requested information on Passport's coding policies and payment policies is available on the MolinaHealthcare.com website under the Policies tab. Questions can be directed to your Passport Provider relations representative.

Reimbursement Guidance and Payment Guidelines

Providers are responsible for the submission of accurate Claims. Passport requires coding of both diagnoses and procedures for all Claims as follows:

- For diagnoses, the required coding schemes are the International Classification of Diseases, 10th Revision, Clinical Modification (ICD-10-CM), if applicable.
- For procedures:
  - Professional and outpatient Claims require the Healthcare Common Procedure Coding System and/or Current Dental Terminology.

Furthermore, Passport requires that all Claims be coded in accordance with the HIPAA transaction code set guidelines and follow the guidelines within each code set.

Passport utilizes a Claim adjudication system that encompasses edits and audits that follow state and federal requirements as well as administers payment rules based on generally accepted principles of correct coding. These payment rules include, but are not limited to, the following:

- Manuals and files published by CMS, including:
    - NCCI edits, including procedure to procedure (PTP) bundling edits and Medically Unlikely Edits (MUE). In the event a state benefit limit is more stringent/restrictive than a federal MUE, Passport will apply the state benefit limit. Furthermore, if a professional organization has a more stringent/restrictive standard than a federal MUE or state benefit limit the professional organization standard may be used.
    - In the absence of state guidance, Medicare National Coverage Determinations (NCD)
    - In the absence of state guidance, Medicare Local Coverage Determinations (LCD)
    - Dental Fee Schedule
    - CDT guidance published by the ADA
    - ICD-10 guidance published by the National Center for Health Statistics
    - State-specific Claim reimbursement guidance
    - Other coding guidelines published by industry-recognized resources
    - Payment policies based on professional associations or other industry-recognized guidance for specific services. Such payment policies may be more stringent than state and federal guidelines.
    - Passport policies based on the appropriateness of Healthcare and medical necessity
    - Payment policies published by Passport

National Correct Coding Initiative (NCCI)

CMS has directed all federal agencies to implement NCCI as policy in support of Section 6507 of the ACA. Passport uses NCCI standard payment methodologies.

NCCI procedure to procedure edits prevent inappropriate payment of services that should not be bundled or billed together and to promote correct coding practices. Based on the NCCI coding manual and CDT guidelines, some services/procedures performed in conjunction with an evaluation and management (E&M) code will bundle into the procedure when performed by the same Provider and separate reimbursement will not be allowed if the sole purpose for the visit is to perform the procedures. NCCI editing also includes MUE which prevent payment for an inappropriate number/quantity of the same service on a single day. An MUE for a HCPCS/CDT code is the maximum number of units of service under most circumstances reportable by the same Provider for the same patient on the same date of service. Providers

must correctly report the most comprehensive CDT code that describes the service performed, including the most appropriate modifier when required.

General Coding Requirements

Correct coding is required to properly process Claims. Passport requires that all Claims be coded in accordance with the HIPAA transaction code set guidelines and follow the guidelines within each code set.

CDT and HCPCS Codes

Codes must be submitted in accordance with the chapter and code-specific guidelines set forth in the current/applicable version of the ADA CDT and HCPCS codebooks. To ensure proper and timely reimbursement, codes must be effective on the date of service for which the procedure or service was rendered and not the date of submission.

ICD-10-CM

Passport utilizes ICD-10-CM and ICD-10-PCS billing rules and will deny claims that do not meet Passport's ICD-10 Claim submission guidelines, if applicable. To ensure proper and timely reimbursement, codes must be effective on the date of service for which the procedure or service was rendered and not the date of submission. Refer to the ICD-10 CM Official Guidelines for Coding and Reporting on the proper assignment of principal and additional diagnosis codes.

Place of Service (POS) Codes

POS codes are two (2)-digit codes placed on Healthcare professional Claims (ADA Claim Form) to indicate the setting in which a service was provided. CMS maintains POS codes used throughout the Healthcare industry. The POS code should be indicative of where that specific procedure/service was rendered. If billing multiple lines, each line should indicate the POS code for the procedure/service on that line.

Coding Sources

Definitions

CDT – Current Dental Terminology; the American Dental Association (ADA) maintained uniform coding system consisting of descriptive terms and codes that are used primarily to identify Dental services and procedures furnished by Providers and other Healthcare professionals.

HCPCS – HealthCare Common Procedural Coding System; a CMS maintained uniform coding system consisting of descriptive terms and codes that are used primarily to identify procedure, supply and durable medical equipment codes furnished by Providers and other Healthcare professionals.

ICD-10-CM – International Classification of Diseases, 10th revision, Clinical Modification ICD-10-CM diagnosis codes are maintained by the National Center for Health Statistics, Centers for Disease Control (CDC) within the Department of Health and Human Services (HHS).

Claim Auditing

Passport shall use established industry Claims adjudication and/or clinical practices, state and federal guidelines, and/or Passport's policies and data to determine the appropriateness of the billing, coding, and payment.

The Provider acknowledges Passport's right to conduct pre- and post-payment billing audits. The Provider shall cooperate with Passport's SIU and audits of Claims and payments by providing access at reasonable times to requested Claims information, the Provider's charging policies and other related data as deemed relevant to support the transactions billed. Additionally, Providers are required, by contract and in accordance with the Provider Manual, to submit all supporting medical records/documentation as requested. Failure to do so in a timely manner may result in an audit failure and/or denial, resulting in an overpayment.

In reviewing medical records for a procedure, Passport reserves the right and where unprohibited by regulation, to select a statistically valid random sample or smaller subset of the statistically valid random sample. This gives an estimate of the proportion of Claims Passport paid in error. The estimated proportion or error rate may be extrapolated across all Claims to determine the amount of overpayment.

Provider audits may be telephonic, an on-site visit, internal claims review, client-directed/regulatory investigation and/or compliance reviews and may be vendor-assisted. Passport asks that you provide Passport or Passport's designee, during normal business hours, access to examine, audit, scan and copy all records necessary to determine compliance and accuracy of billing.

If Passport's Special Investigations Unit suspects that there is fraudulent or abusive activity, Passport may conduct an on-site audit without notice. Should you refuse to allow access to your facilities, Passport reserves the right to recover the full amount paid or due to you.

Timely Claim Processing

Claim processing will be completed for contracted Providers in accordance with the timeliness provisions set forth in the Provider Agreement with Passport. Unless the Provider and Passport have agreed in writing to an alternate schedule, Passport will process the claim for service within 30 days after receipt of Clean Claims.

The receipt date of a Claim is the date Passport receives notice of the Claim.

Electronic Claim Payment

Participating Providers are encouraged to enroll for EFT and ERA. Providers who enroll in EFT payments will automatically receive ERAs as well. EFT/ERA services allow Providers to reduce paperwork, provides searchable ERAs and Providers receive payment and ERA access faster than the paper check and RA processes. There is no cost to the Provider for EFT enrollment and Providers are not required to be in-network to enroll. Passport uses a vendor to facilitate the HIPAA compliant EFT payment and ERA delivery. Additional information about EFT/ERA is available at MolinaHealthcare.com or by contacting the Passport Provider Contact Center.

Overpayments and Incorrect Payments Refund Requests

If, because of retroactive review of Claim payment, Passport determines that it has made an Overpayment to a Provider for services rendered to a Member, it will make a Claim for such Overpayment. Providers will receive an overpayment request letter if the overpayment is identified in accordance with State and CMS guidelines. Providers will be given the option to either:

1. Submit a refund to satisfy overpayment,
2. Submit request to offset from future claim payments, or
3. Dispute overpayment findings.

A copy of the overpayment request letter and details are available in the Availity Provider Portal. In the Overpayment Application section, Providers can make an inquiry, contest, and overpayment with supporting documentation, resolve and overpayment, or check status. This is Passport's preferred method of communication.

Instructions will be provided on the overpayment notice and overpayments will be adjusted and reflected in your remittance advice. The letter timeframes are Passport standards and may vary depending on applicable state guidelines and contractual terms.

Overpayments related to TPL/COB will contain primary insurer information necessary for rebilling including the policy number, effective date, term date, and subscriber information. For members with Commercial COB, Passport will pursue reclamation billing for identified overpayments if the primary insurer is a Commercial payer, in which Passport will seek reimbursement of funds directly from the primary payer. Providers will not receive an overpayment request letter in these scenarios pursuant to state guidelines for commercial recoveries. For members with Medicare COB Passport will provide notice within 540 days from the claim's paid date if the primary insurer is a Medicare plan. A provider may resubmit the claim with an attached primary EOB after submission to the primary payer for payment. Passport will adjudicate the claim and pay or deny the claim in accordance with claim processing guidelines.

A Provider shall pay a Claim for an Overpayment made by Passport which the Provider does not contest or dispute within the specified number of days on the refund request letter mailed to the Provider. If a Provider does not repay or dispute the overpaid amount within the timeframe

allowed Passport may offset the overpayment amount(s) against future payments made to the Provider.

Payment of a Claim for Overpayment is considered made on the date payment was received or electronically transferred or otherwise delivered to Passport, or the date that the Provider receives a payment from Passport that reduces or deducts the overpayment.

Claim Disputes/Reconsiderations/Appeals

Information on Claim disputes/reconsiderations/appeals is in the **Complaints, Grievance, and Appeals Process** section of this Provider Manual.

Balance Billing

The Provider is responsible for verifying eligibility and obtaining approval for those services that require prior authorization.

Providers agree that under no circumstance shall a Member be liable to the Provider for any sums that are the legal obligation of Passport to the Provider. Balance billing a Member for covered services is prohibited, except for the Member's applicable co-payment, coinsurance, and deductible amounts.

Fraud, Waste, and Abuse

Failure to report instances of suspected fraud, waste and abuse is a violation of the law and subject to the penalties provided by law. For additional information please refer to the **Compliance** section of this Provider Manual.

Encounter Data

Each Provider, capitated Provider or organization delegated for Claims processing is required to submit Encounter data to Passport for all adjudicated Claims. The data is used for many purposes, such as regulatory reporting, rate setting and risk adjustment, hospital rate setting, the QI Program and HEDIS® reporting.

Encounter data must be submitted at least weekly and within 30 days from the date of service to meet state and CMS Encounter submission threshold and quality measures. Encounter data must be submitted via HIPAA-compliant transactions, including the ANSI X12N 837I – Institutional, 837P – Professional and 837D – Dental. Data must be submitted with Claims level detail for all non-institutional services provided.

Passport has a comprehensive automated and integrated Encounter data system capable of Supporting all 837 file formats and proprietary formats if needed.

Providers must correct and resubmit any encounters which are rejected (non-HIPAA compliant) or denied by Passport. Encounters must be corrected and resubmitted within 15 days from the rejection/denial.

Passport created 837P, 837I, and 837D Companion Guides with the specific submission requirements available to Providers.

When Encounters are filed electronically Providers should receive two (2) types of responses:

- First, Passport will provide a 999 acknowledgement of the transmission.
- Second, Passport will provide a 277CA response file for each transaction.

12. Complaints, Grievances, and Appeals

Definitions

Grievance**:** A complaint is any oral or written expression of dissatisfaction by an enrollee submitted to the health plan or to a state agency and resolved by close of business the following day. Possible subjects for complaints include, but are not limited to, the quality of care, the quality of services provided, aspects of interpersonal relationships such as rudeness of a provider or health plan employee, failure to respect the enrollee's rights, health plan administration, claims practices, or provision of services that relates to the quality of care rendered by a provider pursuant to the health plan's contract. Possible subjects for grievances include but are not limited to the quality of care, the quality of services provided and aspects of interpersonal relationships such as rudeness of a provider or health plan employee or failure to respect the enrollee's rights.

Appeal: A formal request from an enrollee to seek a review of an action taken by the Plan pursuant to 42 CFR 438.400(b). An appeal is a request for review of an action.

Expedited Appeal: An expedited request for review of an action. An Expedited appeal should be processed when it is determined that allowing the time for a standard resolution could seriously jeopardize the member's life, health, or ability to attain, maintain, or regain maximum function. Such determination is based on:

- A request from the Member
- A provider's support of a member's request
- A provider's request on behalf of the member or
- The plans' determination.

Member Grievance

A patient has the right to express grievances regarding any violation of his or her rights, as stated in Kentucky law, through the grievance process of the dental care provider or dental care facility which served him or her and to the appropriate state licensing agency.

SKYGEN assists Passport with the grievance process. Members are directed to send their grievances to Passport. Providers acting on behalf of the member would also submit their grievance to Passport. Passport will contact Molina Dental Services (MDS) for assistance to resolve the grievance.

For grievances received from the member or the Provider acting on the member's behalf, SKYGEN communicates the recommendation to Passport. Passport will communicate the resolution to the member. SKYGEN will communicate the resolution directly to the provider when the provider is acting on their own behalf. The grievance will be closed and maintained on file for tracking and trending purposes.

Provider Appeals

Providers acting on their own behalf are defined as those who dispute Adverse Determinations when the services have already been provided to the member. Providers are encouraged to submit claim appeals via the SKYGEN Dental HUB or verbally.

Post-Service or claim payment appeal requests, the provider is acting on their own behalf. The appeal should be submitted to SKYGEN within (60) days of the denial. This can be done by submitting a request for appeal in writing with a narrative and supporting documentation to the SKYGEN Provider Appeals Coordinator via mail or the SKYGEN Dental Hub. SKYGEN will resolve the appeal within thirty (30) calendar days of receipt, unless a fourteen (14)-day extension is requested and granted. The appeal timeframe could vary based on appeal contract guidelines.

All provider claim disputes/reconsideration appeals should be sent to:

Provider Appeals
P.O. Box 649
Milwaukee, WI 53201

All prior authorization appeals should be sent to:

Appeals and Grievances Molina Healthcare
P.O. Box 36030
Louisville, KY 40233-6030

Grievance Timeline

A Grievance specialist will conduct the review and will mail a resolution letter to the Member within 30 calendar days from the date the Grievance is received by Passport. The resolution letter may not take the place of the acknowledgement letter, unless a decision is reached

before the acknowledgement letter is sent, then one letter shall be sent which includes the acknowledgement and the decision letter.

Member Standard Appeal Process and Timeline

The Appeal must be received verbally or in writing within 60 calendar days of the date of the Adverse Action. If an Appeal is filed verbally via Passport's Contact Center, the request must be followed up with a written, signed Appeal to Passport within 10 calendar days of the verbal filing. For verbal filings, the time frames for resolution begin on the date the verbal filing was received by Passport. Unless written confirmation of a standard verbal Appeal request is received, the case is closed as an upheld Appeal, and Appeal rights are exhausted. The written follow-up requirement does not apply to qualifying Expedited Appeal requests. An acknowledgement letter will be sent to the Member no later than five (5) days after the Appeal is received, confirming receipt and providing the expected date of resolution. An Appeal Specialist will ensure the appeal is reviewed as expeditiously as the Member's health condition requires. A resolution letter to the Member will be mailed no later than 30 calendar days from the receipt of the Appeal unless the Member requests a 14-calendar-day extension. Passport may also request a 14-day extension when it can show that there is a need for additional information, and it will be in the Member's best interest. If Passport requests an extension, we will give the Member written notice and the extension reason for the extension within two working days of the decision to take an extension. If the Provider files an Appeal on the Member's behalf, Passport will respond to the Provider. The Provider shall give a copy of the notice to the Member or inform the Member of the provisions of the notice.

Expedited Appeal Process and Timeline

An Appeal will be expedited in response to the clinical urgency of the situation, i.e., when a delay would jeopardize a Member's life or materially jeopardize a Member's health. A request to expedite may come from the Member, Member's representative, or a Provider with the Member's written consent. If an appeal request qualifies for expedited, written member consent will not be required.

An expedited Appeal will be acted on quickly and a decision will be made within 72 hours from the date the Appeal request is received either verbally or in writing. If we determine the request does not meet the Commonwealth's definition of an expedited Appeal we will immediately transfer the Appeal to the process and timeframes for a Standard Appeal resolution, in which a 30-day period will begin on the date we receive the original Appeal request, and we'll also notify the Member within two calendar days.

External Independent Review

In accordance with 907 KAR 17:035, if a Provider receives an adverse final decision of a denial, in whole or in part, of a health service [including a denial, in whole or in part, involving Emergency Services or Claim for reimbursement related to this service, the Provider may

request an external independent third-party review. A Provider may only do so after first completing an internal Appeal process with Passport by Molina Healthcare. A request for external independent third-party review must be submitted to Passport by Molina Healthcare within 60 days of receiving the final partially overturned or upheld appeal decision letter from us. If a Provider has not received a final appeal decision letter outlining the external independent third-party review rights, your internal appeal must be completed prior to the external independent third-party review submission.

Requests for external independent third-party reviews may be submitted to Passport by Molina Healthcare via one of the following methods:

- E-mail: ReviewRequests@MolinaHealthcare.com
- Fax: (502) 585-8334
- Passport by Molina Healthcare
  Attention: External Independent Third-Party Review Request
  PO Box 36030
  Louisville, KY 40233

Passport will confirm receipt of your request for external independent third-party review within five business days of receiving your request. As requested by 907 KAR 17:035, if you request an external independent third-party review, we will forward to the Department for Medicaid Services all documentation submitted by you during the Appeal process within 15 business days of receiving your request. No additional documentation will be allowed for consideration by the external independent third-party review.

Additionally, if Passport's decision is upheld by the external independent third-party review, Providers have the right to request an administrative hearing in accordance with 907 KAR 17:040 within 30 calendar days of the Department's written notice. You must submit your request for administrative hearing to:

Department for Medicaid Services, Appeals and Complaints Branch
Attention: Administrative Hearings
275 E. Main Street, Mail Stop 6E-D
Frankfort, KY 40621

If the administrative hearing officer upholds Passport's decision, the Provider must reimburse the Department for Medicaid Services in the amount of $600.00 (per hearing) within thirty (30) days of the issuance of the final order.

Reporting

Grievance and appeal trends are reported to the Quality Improvement and Health Equity Transformation Committee quarterly. This trend report includes a quantitative review of trends, qualitative or barriers analysis and identification of interventions that address key

drivers. An annual evaluation of grievance and appeal analysis is then completed and presented to the Quality Improvement and Health Equity Transformation Committee for evaluation. If required by the state or CMS, reporting is submitted to the appropriate agency as needed.

13. Network Participation

Dental Provider Credentialing and Recredentialing

Molina Dental Services, in partnership with SKYGEN, invites you to become a Participating dental Provider administering Passport by Molina Healthcare dental benefits to Kentucky Members. SKYGEN verifies all information on the Provider Application prior to contracting and re-verifies this information every three years. The information is then presented to the Professional Review Committee to evaluate a Provider's qualifications to participate in the Molina Dental network.

The purpose of the Credentialing Program is to assure that Molina Dental Services, in partnership with SKYGEN, and its subsidiaries (Molina) network consists of quality Providers who meet clearly defined criteria and standards. It is the objective of Molina Dental Services to provide superior oral health care to the community.

The decision to accept or deny a credentialing applicant is based upon primary source verification, secondary source verification and additional information as required. The information gathered is confidential and disclosure is limited to parties who are legally permitted to have access to the information under State and Federal Law.

The Credentialing Program has been developed in accordance with State and Federal requirements. In addition, Molina Dental Services, in partnership with SKYGEN, utilizes the current National Committee for Quality Assurance (NCQA) Standards and Guidelines for the Accreditation of MCOs for the credentialing and re-credentialing of licensed independent providers and provider groups with whom/which it contracts or employs and who fall within its scope of authority and action. The Credentialing Program is reviewed annually, revised, and updated as needed.

Please note for the current process, you must be enrolled as a Kentucky Medicaid Provider and have an active Medicaid ID and a National Provider Identifier Standard (NPI). Review and sign the Dental Provider Service Agreement.

Each Provider will be required to complete credentialing in one of following ways:

- Email your Council for Affordable Quality Healthcare (CAQH) ProView ID to the credentialing team at credentialing@skygenusa.com
- A CAQH ProView ID can be obtained at: https://proview.caqh.org/PR/Registration.
- CAQH must be reattested within the last 4 months by visiting https://proview.caqh.org

- Indicate “global” authorization which allows access to your data profile to all healthcare organizations. Provider may upload copies of their current DEA license and malpractice insurance copy directly to CAQH
- Submitting a paper application

Non-Discriminatory Credentialing and Recredentialing

Molina Dental Services, in partnership with SKYGEN, does not make credentialing and recredentialing decisions based on an applicant’s race, ethnic/national identity, gender, gender identity, age, sexual orientation, ancestry, religion, marital status, health status, or high-risk patient types (e.g., Medicaid), or costly treatment for conditions in which the practitioner specializes. If Molina Dental Services, in partnership with SKYGEN, declines to include individual or group providers in its network, it will give the affected providers written notice of the reason for its decision, per Federal requirements at 42 CFR § 438.12(b)This does not mean that Molina Dental Services, in partnership with SKYGEN, is required to contract with providers beyond the number necessary to meet the needs of its members; does not preclude Molina Dental Services from including in its network practitioners who meet certain demographic or specialty needs, for example, to meet cultural needs of Members; and does not preclude Molina Dental Services from using different reimbursement amounts for different specialties or for different practitioners in the same specialty; and does not preclude the MCO from establishing measures that are designed to maintain quality of services and control costs and is consistent with its responsibilities to its members.

Credentialing Turnaround Time

Molina Dental Services, in partnership with SKYGEN, will completely process applications from all provider types within 30 days of receipt of a complete application. A complete credentialing application includes all necessary documentation and attachments. “Completely process” means that Molina must:

- Review, approve, and load approved providers to its provider files in its system and submit the information in the weekly electronic provider file to Passport or Passport’s designee; or
- Deny the application and ensure that the provider is not used by Molina Dental Services.

Criteria for Participation in the Passport Network

Molina Dental Services, in partnership with SKYGEN, has established criteria and the sources used to verify these criteria for the evaluation and selection of practitioners for participation in the Passport network. These criteria have been designed to assess a Practitioner’s ability to deliver care. This policy defines the criteria that are applied to applicants for initial participation, recredentialing and ongoing participation in the Passport network. To remain eligible for participation, Practitioners must continue to satisfy all applicable requirements for participation as stated herein and in all other documentation provided by Passport.

Molina Dental Services, in partnership with SKYGEN, reserves the right to exercise discretion in applying any criteria and to exclude Practitioners who do not meet the criteria. Passport may, after considering the recommendations of the Professional Review Committee, waive any of the requirements for network participation established pursuant to these policies for good cause if it is determined such waiver is necessary to meet the needs of Molina Dental Services and the community it serves. The refusal of Molina Dental Services, in partnership with SKYGEN, to waive any requirement shall not entitle any Practitioner to a hearing or any other rights of review.

Providers shall not be eligible to see Passport Members as Participating Providers until notified of their effective date from Molina Dental Services, in partnership with SKYGEN.

Additionally, Providers shall not be eligible to treat Members as a Participating Provider at a location until both notified of credentialing completion and added to the Health Plan systems. The Provider will receive a welcome notice from SKYGEN with the effective date of participation.

Practitioners must meet the following criteria to be eligible to participate in the Molina Dental network. The Practitioner shall have the burden of producing adequate information to prove they meet all criteria for initial participation and continued participation in the Molina Dental network. If the Practitioner does not provide this information, the credentialing application will be deemed incomplete and a discontinue notice will be sent.

- **Application** –Practitioners must submit to Molina Dental Services, in partnership with SKYGEN, a complete credentialing application either from CAQH ProView or a standard practitioner application. The attestation must be signed within 120 days. Application must include all required attachments.
- **License, Certification or Registration** –Practitioners must hold a current and valid license, certification, or registration to practice in their specialty in every State in which they will provide care and/or render services for Passport Members. Telemedicine Practitioners are required to be licensed in the State where they are located, and the State the Member is located.
- **DEA or CDS Certificate** –Practitioners must hold a current, valid, unrestricted Drug Enforcement Agency (DEA) or Controlled Dangerous Substances (CDS) certificate. Practitioners must have a DEA or CDS in every State where the Practitioner provides care to Molina Members. If a Practitioner has a pending DEA/CDS certificate and never had any disciplinary action taken related to their DEA and/or CDS or chooses not to have a DEA and/or CDS certificate, the Practitioner must then provide a documented process that allows another Practitioner with a valid DEA and/or CDS certificate to write all prescriptions requiring a DEA number. Practitioners must utilize a prescription drug monitoring program (PDMP) is an electronic database that tracks controlled substance prescriptions in a state. PDMPs can provide health authorities with timely information about prescribing and patient behaviors that contribute to the epidemic and facilitate a nimble and targeted response.

- **Specialty** –Practitioners must only be credentialed in the specialty in which they have adequate education and training. Practitioners must confine their practice to their credentialed area of practice when providing services to Passport Members.
- **Education** – Practitioners must have graduated from an accredited school with a degree required to practice in their designated specialty.
- **Board Certification** – Board certification in the specialty in which the Practitioner is practicing is not required.
- **Work History** –Practitioners must supply the most recent five years of relevant work history on the application or curriculum vitae. Relevant work history includes work as a health professional. If a gap in employment exceeds six months, the Practitioner must clarify the gap verbally or in writing. The organization will document verbal clarification in the Practitioner's credentialing file. If the gap in employment exceeds one year, the Practitioner must clarify the gap in writing.
- **Malpractice History** –Practitioners must supply a history of malpractice and professional liability claims and settlement history in accordance with the application. Documentation of malpractice and professional liability claims, and settlement history is requested from the Practitioner on the credentialing application. If there is an affirmative response to the related disclosure questions on the application, a detailed response is required from the Practitioner.
- **State Sanctions, Restrictions on Licensure or Limitations on Scope of Practice** – Practitioners must disclose a full history of all license/certification/registration actions including denials, revocations, terminations, suspension, restrictions, reductions, limitations, sanctions, probations, and non-renewals. Practitioners must also disclose any history of voluntarily or involuntarily relinquishing, withdrawing, or failure to proceed with an application to avoid an adverse action, or to preclude an investigation or while under investigation relating to professional competence or conduct. If there is an affirmative response to the related disclosure questions on the application, a detailed response is required from the Practitioner. At the time of initial application, the Practitioner must not have any pending or open investigations from any State or governmental professional disciplinary body[3]. This would include Statement of Charges, Notice of Proposed Disciplinary Action, or the equivalent.
- **Medicare, Medicaid and other Sanctions and Exclusions** – Practitioners must not be currently sanctioned, excluded, expelled, or suspended from any State or Federally funded program including but not limited to the Medicare or Medicaid programs. Practitioners must disclose all Medicare and Medicaid sanctions. If there is an affirmative response to the related disclosure questions on the application, a detailed response is required from the Practitioner. Practitioners must disclose all debarments,

[3] If a practitioner's application is denied solely because a practitioner has a pending Statement of Charges, Notice of Proposed Disciplinary Action, Notice of Agency Action or the equivalent from any state or governmental professional disciplinary body, the practitioner may reapply as soon as practitioner is able to demonstrate that any pending Statement of Charges, Notice of Proposed Disciplinary Action, Notice of Agency Action, or the equivalent from any state or governmental professional disciplinary body is resolved, even if the application is received less than one year from the date of original denial.

suspensions, proposals for debarments, exclusions, or disqualifications under the non-procurement common rule, or when otherwise declared ineligible from receiving Federal contracts, certain subcontracts, and certain Federal assistance and benefits. If there is an affirmative response to the related disclosure questions on the application, a detailed response is required from the Practitioner.

- **Social Security Administration Death Master File** – Practitioners must provide their Social Security number. That Social Security number should not be listed on the Social Security Administration Death Master File.
- **Medicare Preclusion List** – Practitioners currently listed on the Preclusion List may not participate in the Molina network for any Medicare or Duals (Medicare/Medicaid) lines of business.
- **Professional Liability Insurance** – Practitioners must have and maintain professional malpractice liability insurance with limits that meet Passport criteria. This coverage shall extend to Passport Members and the Practitioners activities on Passport's behalf. Practitioners maintaining coverage under Federal tort or self-insured policies are not required to include amounts of coverage on their application for professional or dental malpractice insurance.
- **Inability to Perform** – Practitioners must disclose any inability to perform essential functions of a Practitioner in their area of practice with or without reasonable accommodation. If there is an affirmative response to the related disclosure questions on the application, a detailed response is required from the Practitioner.
- **Lack of Present Illegal Drug Use** – Practitioners must disclose if they are currently using any illegal drugs/substances.
- **Criminal Convictions** – Practitioners must disclose if they have ever had any of the following:
    - Criminal convictions, including any convictions, guilty pleas, or adjudicated pretrial diversions for crimes against person such as murder, rape, assault, and other similar crimes.
    - Financial crimes such as extortion, embezzlement, income tax evasion, insurance fraud, and other similar crimes.
    - Any crime that placed the Medicaid or Medicare program or its beneficiaries at immediate risk, such as a malpractice suit which results in a conviction of criminal neglect or misconduct.
    - Any crime that would result in mandatory exclusion under section 1128 of the Social Security Act.
    - Any crime related to fraud, kickbacks, health care fraud, claims for excessive charges, unnecessary services or services which fail to meet professionally recognized standards of health care, patient abuse or neglect, controlled substances, or similar crimes.
    - At the time of initial credentialing, practitioner must not have any pending criminal charges in the categories listed above.

At the time of initial credentialing, practitioners must not have any pending criminal charges in the categories listed above.

- **Loss or limitations of clinical privileges** – At initial credentialing, Practitioners must disclose all past and present issues regarding loss or limitation of clinical privileges at all facilities or organizations with which the Practitioner has had privileges. If there is an affirmative response to the related disclosure questions on the application, a detailed response is required from the Practitioner. At recredentialing, Practitioners must disclose past and present issues regarding loss or limitation of clinical privileges at all facilities or organizations with which the Practitioner has had privileges since the previous credentialing cycle.
- **Hospital privileges** – Practitioners must list all current hospital privileges on their credentialing application. If the Practitioner has current privileges, they must be in good standing.
- **National Provider Identifier (NPI)** – Practitioners must have an NPI issued by CMS.

Notification of Discrepancies in Credentialing Information and Practitioner's Right to Correct

Molina Dental Services, in partnership with SKYGEN, will notify the Practitioner immediately in writing if credentialing information obtained from other sources varies substantially from that provided by the Practitioner. Examples include but are not limited to actions on a license, malpractice claims history, board certification actions, sanctions, or exclusions. Molina Dental Services, in partnership with SKYGEN, is not required to reveal the source of information if the information is obtained to meet organization credentialing verification requirements or if disclosure is prohibited by law.

Practitioners have the right to correct erroneous information in their credentials file. Practitioner's rights are published on the Passport website and are included in this Dental Provider Manual. The notification sent to the Practitioner will detail the information in question and will include instructions to the Practitioner indicating:

Their requirement to submit a written response within 10 calendar days of receiving notification from Molina Dental Services, in partnership with SKYGEN. In their response, the Practitioner must explain the discrepancy, may correct any erroneous information, and may provide any proof that is available. The Practitioner's response must be sent to SKYGEN Credentialing at:

Fax: 866.396.5686
Email: credentialing@skygenUSA.com

Upon receipt of notification from the Practitioner, SKYGEN will document receipt of the information in the Practitioner's credentials file. SKYGEN will then re-verify the primary source information in dispute. If the primary source information has changed, correction will be made immediately to the Practitioner's credentials file. The Practitioner will be notified in writing that the correction has been made to their credentials file. If the primary source information remains inconsistent with the Practitioner's information, SKYGEN will notify the Practitioner.

If the Practitioner does not respond within 10 calendar days, their application processing will be discontinued, and network participation will be administratively denied or terminated.

Practitioner's Right to Review Information Submitted with the Credentialing Application

Practitioners have the right to review their credentials file at any time. Practitioner's rights are published on the Molina website and are included in this Dental Provider Manual. The Practitioner must notify SKYGEN and request an appointment time to review their file and allow up to seven calendar days to coordinate schedules. The Dental Director and the Director responsible for Credentialing or the Quality Improvement Director will be present. The Practitioner has the right to review all information in the credentials file except peer references or recommendations protected by Law from disclosure.

The only items in the file that may be copied by the Practitioner are documents which the Practitioner sent to SKYGEN (e.g., the application and any other attachments submitted with the application from the Practitioner). Practitioners may not copy any other documents from the credentialing file.

Practitioner's Right to be Informed of the Application Status

Practitioners have the right, upon request, to be informed of the status of their application by telephone, email, or mail. Practitioner's rights are published on the Molina website and are included in this Dental Provider Manual. SKYGEN will respond to the request within two working days. SKYGEN will share with the Practitioner where the application is in the credentialing process and note any missing information or information not yet verified.

Notification of Credentialing Decisions

Initial credentialing decisions are communicated to Practitioners via letter or email. This notification is typically sent by the SKYGEN Dental Director within two weeks of the decision. Under no circumstance will notifications letters be sent to the Practitioners later than 30 calendar days from the decision. Notification of recredentialing approvals is not required.

Recredentialing

SKYGEN recredentials every Practitioner at least every 36 months. Providers will receive notification 6 months in advance. SKYGEN follows NCQA guidelines for re-credentialing. All re-credentialing applications must be completely approved before the lapse date to avoid any claim or payment impact. For additional information, please email credentialing@skygenUSA.com

Excluded Providers

Excluded Provider means an individual Provider, or an entity with an officer, director, agent, manager, or individual who owns or has a controlling interest in the entity who has been convicted of crimes as specified in Section 1128 of the Social Security Act, and excluded from participation in the Medicare or Medicaid program; assessed a civil penalty under the provisions of section 1128, or has a contractual relationship with an entity convicted of a crime specified in section 1128.

Pursuant to section 1128 of the SSA, Molina Dental Services, in partnership with SKYGEN, may not subcontract with an Excluded Provider/person. Molina Dental Services, in partnership with SKYGEN, shall terminate subcontracts immediately when Molina Dental Services, in partnership with SKYGEN, become aware of such excluded Provider/person or when Molina Dental Services, in partnership with SKYGEN, receive notice. Molina Dental Services, in partnership with SKYGEN, certify that neither it nor its Provider is presently debarred, suspended, proposed for debarment, declared ineligible, or otherwise excluded from participation in any State or Federal program; or is an individual or entity listed on the Federal System for Award Management, the Office of Inspector General's List of Excluded Individuals and Entities database, or the Kentucky Medicaid Excluded Providers.

Ongoing Monitoring of Sanctions and Exclusions

SKYGEN monitors the following agencies for Practitioner sanctions and exclusions between recredentialing cycles for all Practitioner types and takes appropriate action against Providers when instances of poor quality are identified. If a Passport Practitioner is found to be sanctioned or excluded, the Provider's contract will be immediately terminated effective the same date as the sanction or exclusion was implemented.

- **The United States Department of Health & Human Services (HHS), Office of Inspector General (OIG) Fraud Prevention and Detection Exclusions Program** – Monitor for individuals and entities that have been excluded from Medicare and Medicaid programs.
- **The OIG High Risk List** – Monitor for individuals or facilities who refused to enter a Corporate Integrity Agreement (CIA) with the federal government on or after October 1, 2018.
- **State Medicaid exclusions** – Monitor for state Medicaid exclusions through each state's specific Program Integrity Unit (or equivalent).
- **Medicare Exclusion Database (MED)** – Monitor for Medicare exclusions through the CMS MED online application site.
- **Medicare Preclusion List** – Monitor for individuals and entities that are reported on the Medicare Preclusion List.
- **National Practitioner Database (NPDB)** – Passport enrolls all credentialed practitioners with the NPDB Continuous Query service to monitor for adverse actions on license, DEA, hospital privileges and malpractice history between credentialing cycles.
- **System for Award Management (SAM)** – Monitor for Practitioners sanctioned by SAM.

SKYGEN also monitors the following for all Practitioner types between the credentialing cycles.

- Member complaints/grievances
- Adverse events
- Social Security Administration Death Master File

Provider Appeal Rights

In cases where the Professional Review Committee suspends or terminates a Practitioner's contract based on quality of care or professional conduct, a certified letter is sent to the Practitioner describing the adverse action taken and the reason for the action, including notification to the Practitioner of the right to a fair hearing when required pursuant to laws or regulations.

14. Delegation

Delegation is a process that gives another entity the ability to perform specific functions on behalf of Passport. Passport may delegate:

- Utilization management
- Credentialing and recredentialing
- Claims
- Complex case management
- CMS Preclusion List monitoring
- Other clinical and administrative functions

When Passport delegates any clinical or administrative functions, Passport remains responsible to external regulatory agencies and other entities for the performance of the delegated activities, including functions that may be sub-delegated. To become a delegate, the Provider/accountable care organization (ACO)/vendor must be in compliance with Passport's established delegation criteria and standards. Passport's Delegation Oversight Committee (DOC) or other designated committee must approve all delegation and sub-delegation arrangements. To remain a delegate, the Provider/ACO/vendor must maintain compliance with Passport's standards and best practices.

Delegation Reporting Requirements

Delegated entities contracted with Passport must submit monthly and quarterly reports. Such reports will be determined by the function(s) delegated and will be reviewed by Passport delegation oversight staff for compliance with performance expectations within the timeline indicated by Passport.

Corrective Action Plans and Revocation of Delegated Activities

If it is determined that the delegate is out of compliance with Passport's guidelines or regulatory requirements, Passport may require the delegate to develop a corrective action plan designed to bring the delegate into compliance. Passport may also revoke delegated activities if

it is determined that the delegate cannot achieve compliance or if Passport determines that is the best course of action.

If you have additional questions related to delegated functions, please contact your Passport Contract Manager.

15. Pharmacy

Prescription drug therapy is an integral component of your patient's comprehensive treatment program. Passport's goal is to provide our Members with high-quality, cost-effective drug therapy. Passport works with our Providers to ensure medications used to treat a variety of conditions and diseases are offered. Passport covers prescription and certain over-the-counter drugs.

Pharmacy Network

Members must use their Passport Member ID card to get prescriptions filled. Passport's network includes retail, mail, long term care and specialty pharmacies. Additional information regarding the pharmacy benefits, limitations, and network pharmacies is available on Passport's website at MolinaHealthcare.com or by calling Passport at (800) 578-0603.

Member and Provider "Patient Safety Notifications"

Passport has a process to notify Members and Providers regarding a variety of safety issues which include voluntary recalls, FDA-required recalls, and drug withdrawals for patient safety reasons. This is also a requirement as an NCQA-accredited organization.

Pain Safety Initiative (PSI) Resources

Safe and appropriate opioid prescribing and utilization is a priority for all of us in Healthcare. Password requires Providers to adhere to Passport's drug formularies and prescription policies designed to prevent abuse or misuse of high-risk chronic pain medication. Providers are expected to offer additional education and support to Members regarding opioid and pain safety as needed.

Passport is dedicated to ensuring Providers are equipped with additional resources, which can be found on the Passport Provider website. Providers may access additional opioid safety and substance use disorder resources at MolinaHealthcare.com under the Health Resources tab. Please consult with your Provider Services representative or reference the medication formulary for more information on Passport's Pain Safety Initiatives.