blue california

601 12th Street
Oakland, CA 94607

April 23, 2025

Subject: **Notification of July 2025 updates to the Blue Shield *HMO IPA/Medical Group Procedures Manual***

Dear IPA/medical group:

Blue Shield is revising the *HMO IPA/Medical Group Procedures Manual* (Manual). The changes in each provider manual section listed below are effective July 1, 2025.

On that date, you can search and download the revised manual on Provider Connection at www.blueshieldca.com/provider in the *Provider Manuals* section under *Guidelines & resources*.

You may also request a PDF version of the revised *HMO IPA/Medical Group Procedures Manual* be emailed to you once it is published by emailing providermanuals@blueshieldca.com.

The *HMO IPA/Medical Group Procedures Manual* is included by reference in the agreement between Blue Shield of California (Blue Shield) and those IPAs and medical groups contracted with Blue Shield. If a conflict arises between the *HMO IPA/Medical Group Procedures Manual* and the agreement held by the IPA or medical group and Blue Shield, the agreement prevails.

If you have any questions regarding this notice or about the revisions to be published in the July 2025 version of this Manual, please contact your Blue Shield Provider Relations Coordinator.

Sincerely,

Aliza Arjoyan
Senior Vice President
Provider Partnerships and Network Management

Section 2.8: Benefits and Benefit Programs

Care Management

Maternity Management

Deleted and ***replaced*** the following section to comply with AB 1936:

Blue Shield has teamed up with Maven to offer Maven Maternity to our members at no cost. Maven Maternity is a 24/7 digital and virtual program designed to support Blue Shield members during and after pregnancy. Maven is also available to eligible Blue Shield medical plan members and their partners who have experienced a pregnancy loss. Blue Shield members can use Maven to book coaching and educational video appointments with providers across more than 30 specialties, including OB-GYNs, mental health specialists, doulas, lactation consultants, and more at no cost. Providers can encourage members to enroll in the Maven Maternity Program by visiting www.blueshieldca.com/maternity.

Screening for maternal mental health-related conditions is required during pregnancy with at least one additional screening during the first six weeks of the postpartum period. Additional postpartum screenings are strongly encouraged if determined to be medically necessary and clinically appropriate in the judgment of the treating provider. Blue Shield providers may connect a member to appropriate maternal mental health resources through accessing multiple pathways based on member's needs. These include connecting directly to Maven, through Blue Shield Care Management, referring to behavioral health providers through the Blue Shield MHSA, or providers through the Blue Shield of California provider network. Physician referrals are an important component of Blue Shield's Care Management Programs and may allow for identification of a member more quickly.

Providers can refer to Blue Shield Care Management Programs via secure email to bscliaison@optum.com or fax to (877) 280-0179. To download an electronic copy of the referral form, please visit www.blueshieldca.com/provider/guidelines-resources/patient-care/programs.sp. Providers can refer members to Magellan by calling Customer Service at (877) 263-9952 or request a clinical referral form at BSCClinicalLiaison@MagellanHealth.com. Each referral will be evaluated for eligibility and appropriateness.

Section 4.1: Network Administration

Contracting Requirements for Administrative Services Agreements (applies to MSOs or other entities)

Added the following to list of contract provisions that administrative service agreements must contain to comply with NCQA requirements:

- The process by which the IPA/medical group annually evaluates the delegated entity's performance and includes the following:
  - The agreement should include the annual review of the delegate's policies and procedures and review of files, as applicable, and Credentialing Information Integrity (CII) annual audit and monitoring processes.

- The agreement has appropriate language regarding safeguarding the information used in the credentialing and recredentialing processes against inappropriate documentation and updates. The agreement should specify that the following documentation and updates to credentialing are inappropriate:
    1. Falsifying credentialing dates (e.g., licensure date, credentialing decision date, staff verifier date, ongoing monitoring dates).
    2. Fraudulently altering existing documents (e.g., credentialing minutes, clean file reports, ongoing monitoring reports).
    3. Attributing verification or review to an individual who did not perform the activity.
    4. Updates to information by unauthorized individuals.

- Any new agreements effective on or after July 1, 2025, must include NCQA's CII requirements. Prior to July 1, 2025, if the agreement already includes the credentialing system controls requirements, an update is not required. However, if this information was not included, the agreement must be updated with the required NCQA CII language prior to July 1, 2025.

Practitioner Credentialing

Updated the following credentialing criteria per NCQA standards:

1. Board certified by the American Board of Medical Specialties (ABMS) or American Osteopathic Association (AOA) specialty boards; **or**
2. Completed the requisite residency or fellowship required by the ABMS or AOA specialty boards;
7. Be free of any Medical Board of California (MBC) restrictions and Medicare/Medicaid sanctions, exclusions, or any restrictions from their issuing licensing board.
9. Participation as a Blue Shield Medicare Advantage Plan Physician requires that physicians maintain Clinical Laboratory Improvement Amendments (CLIA) certification/waiver certificates for any office lab work performed, participate in the Medicare Program, and be free of Medicare sanctions, exclusions, or restrictions.

Other IPA/Medical Group Responsibilities

Added the following section under the Sensitive Health Information section to comply with AB 2843:

Sensitive Services

"***Sensitive services***" are health care services related to mental or behavioral health, sexual and reproductive health, sexually transmitted infections, substance use disorder, gender affirming care, intimate partner violence, and rape or sexual assault.

Claims submitted for services related to rape and/or sexual assault are excluded from any cost sharing (pursuant to AB 2843). Blue Shield is prohibited from requiring that a police report be filed, for charges to be brought against the assailant, or for an assailant to be convicted; to provide the covered services.

Section 4.2: Member Rights and Responsibilities

Member Grievance Process

Added the following language regarding the use of the AOR form to submit an appeal or grievance on the member's behalf:

The Appointment of Representative (AOR) form is a Blue Shield branded privacy form that allows members to appoint a representative to act on their behalf through the appeals and grievance process. This includes providers, brokers, non-members, and parents of a minor appealing confidential information. This form, or an equivalent, will need to be submitted prior to the requestor being able to submit an appeal or grievance on behalf of the member. A copy of the AOR form can be found on Provider Connection at www.blueshieldca.com/provider under *Guidelines & resources*, *Forms*, then *Patient care forms*.

Section 5.1: Utilization Management

Utilization Management (UM) Criteria and Guidelines

Updated the following resources in boldface type to comply with SB 855:

- Applied Behavior Analysis Practice Guidelines for the Treatment of Autism Spectrum Disorder; Council on Autism Providers (CASP) **as documented in the Blue Shield Medical Policy**
- Psychological and Neuropsychological Testing Billing and Coding Guide; American Psychological Association **as documented in the Blue Shield Medical Policy**

Mental Health and Substance Use Disorder Services

Blue Shield Mental Health Service Administrator (MHSA) Covered Services and Financial Responsibility

Updated language explaining practice guidelines for covered services in boldface type below:

The Blue Shield MHSA will utilize ASAM, LOCUS, CALOCUS, ECSII, **Council of Autism Service Providers ABA Therapy guidelines, American Psychological Association's Neuropsychological Testing guidelines, Canadian Network of Mood and Anxiety Treatment for TMS guidelines, American Psychiatric Association's ECT guidelines, and WPATH guidelines for the treatment of gender dysphoria**. Additional mental health and substance use disorder guidelines may be added as they become available from non-profit professional associations in accordance with California law.

IPA/Medical Group Covered Services and Financial Responsibility

Updated the bullet point describing the guidelines used by IPA/medical group in making UM decisions, in boldface type below:

The IPA/medical group remains responsible for the services listed below even when members' mental health and substance use disorder benefits are being managed by Blue Shield's MHSA:

- Decisions related to delegated medical services. As such, medical services for the treatment of gender dysphoria, eating disorder, or substance use disorder are the responsibility of the IPA/medical group. In making utilization management decisions, the IPA/medical group will utilize **ASAM guidelines, LOCUS guidelines, CALOCUS guidelines, ECSII guidelines, Council of Autism Service Providers ABA Therapy guidelines, American Psychological**

Association's Neuropsychological Testing guidelines, Clinical Guidelines for the Management of Adults with Major Depressive Disorder, Section 4, Canadian Network of Mood and Anxiety Treatment for TMS guidelines, American Psychiatric Association's ECT guidelines, and WPATH guidelines for the treatment of gender dysphoria. Additional MH/SUD guidelines may be added as they become available from non-profit professional associations in accordance with California law.

Section 5.2: Quality Management Programs

Delegation of Credentialing

Credentialing Oversight

Added the following language to this section:

The IPA/medical group will be required to sign and abide by the credentialing delegation agreement.

Added the following language about the Oversight of Credentialling Information Integrity (CII) requirements. These requirements replace NCQA's Credentialing System Controls requirements as of 7/1/25.

4. **Oversight of Credentialing Information Integrity (CII).**
   The IPA/medical group must have policies and procedures addressing the integrity of information used in the credentialing process, conduct audits of credentialing information for inappropriate documentation and updates and implement corrective actions to address identified information integrity issues.

   A. Protecting the Integrity of the information. The IPA/medical group has CII policies and procedures that specify:

      i. The scope of credentialing information. Policies must describe the protection of each of the following documents:

         - Application and attestation
         - Credentialing documents received from primary source or agent
         - Documentation of credentialing activities, to include:
            - Verification dates
            - Report dates
            - Credentialing decisions
            - Credentialing decision dates
            - Signature or initials of the verifier or reviewer
         - Credentialing Committee Minutes
         - Documentation of clean file approval, if applicable
         - Credentialing checklist, if used

      ii. The staff responsible for performing credentialing activities. Policies must include titles of staff who:

         - Document credentialing activities
         - Staff authorized to modify, edit, update, or delete credentialing information
         - Perform the annual oversight of CII functions, including the annual audit and follow-up

      iii. The process for documenting updates to credentialing information, including:

- Description of when it is acceptable to update credentialing information.
- The process staff should follow when making updates to credentialing information including the following documentation:
  - When the information was updated. (date and time)
  - What information was updated
  - Why the information was updated
  - Staff who update the information

iv. The following items are inappropriate updates to credentialing information:
- Falsifying credentialing dates (e.g., licensure date, credentialing decision date, staff verifier date, ongoing monitoring dates)
- Creating documents without performing the required activities (e.g., photocopying a prior credential and updating information as a new credential)
- Fraudulently altering existing documents (e.g., credentialing minutes, clean-file reports, ongoing monitoring reports)
- Attributing verification or review to an individual who did not perform the activity
- Updates to information by unauthorized individuals

v. The auditing, documenting, and reporting of information integrity issues. The policies and procedures must:
- Specify that IPA/medical group audits credentialing staff documentation and updates.
- Describes the process for documenting and reporting inappropriate documentation and updates to:
  - IPA/medical groups designated individual (s) when identified, and
  - Outline consequences for inappropriate documentation and updates to NCQA when it identifies fraud and misconduct.

B. Information Integrity Training: IPA/medical group shall annually train credentialing staff on:

i. Inappropriate documentation and updates related to Element a. iv.

ii. Audits of staff, documenting and reporting information integrity issues for Element a. v.
- Training informs staff of:
  - The audits of staff documentation and updates to credentialing files
  - Process for documenting and reporting inappropriate documentation and updates to the designated individual(s)
  - The consequences for inappropriate documentation and updates.

C. Audit and Analysis.

i. Audit. The IPA/medical group must annually audit credentialing information used in the credentialing process for inappropriate documentation and updates. The IPA/medical group:
- Must provide evidence that an annual CII audit was conducted for:
  - Falsifying credentialing dates (e.g., licensure date, credentialing decision date, staff verifier date, ongoing monitoring dates)
  - Creating documents without performing the required activities (e.g., photocopying a prior credential and updating information as a new credential)
  - Fraudulently altering existing documents (e.g., credentialing minutes, clean-

file reports, ongoing monitoring reports)
    - Attributing verification or review to an individual who did not perform the activity
    - Updates to information by unauthorized individuals
- Audit universe is to include a random sample of 5% or maximum of 50 files. If 5% is less than 20 total files, it is required to do a minimum of 10 initial and 10 recredentialing. Universe to include all initial or recredentialing decisions made during the look-back period (12 months).
- Audit and Analysis report must include the following: report date, title of individuals who conducted the audit, auditing methodology (the auditing period, file universe size, audit sample size), audit log (as referenced attachment) showing file identifier and type of credentialing information audited, findings for each file and rationale, and results (percentages and total inappropriate documentation and updates found)

ii. IPA/medical group annually conducts qualitative analysis of inappropriate documentation and up updates.

- IPA/medical group performs a qualitative analysis for each inappropriate documentation and update found during the audit to determine the cause. The cause is then documented along with staff who performed the qualitative analysis.

D. Improvement Actions

i. Corrective Action. The IPA/medical group must implement corrective actions to address all inappropriate documentation and updates found in Element C.

- Documentation of corrective actions must include actions the IPA/medical group has taken or plans to take, dates of action for all credentialing information found to be inappropriate including title of staff responsible for implementing the corrective measures.
    - Stating annual training as the corrective action may not be the only action. *Example:* The PO's credentialing manager shared the annual audit report/analysis results with proposed actions with the PO's leadership and determined appropriate action and time framed for completion of all corrective actions.

ii. Audit. The IPA/medical group must conduct an audit of the effectiveness of corrective actions on finding 3-6 months after completion of the annual audit in Element C.

- Audit must be conducted 3-6 months after the annual audit to determine if the corrective action measures taken were effective. File universe should be those with credentialing or recredentialing decisions made within the preceding 3-6 months.
- Overall effectiveness – Conclusion. The IPA/medical group should have a statement concluding out the results of the reaudit and if their implemented corrective action measures were or were not effective based on the overall results.

Upon completion of the audit, the IPA/medical group will be notified of their audit results.

Required Submissions/Notifications of Credentialing Program Activity

Added the following bullet point to list of items IPA/medical groups are responsible to notify Blue Shield of:

The IPA/medical group shall keep Blue Shield apprised of credentialing program activity through the following:

- Practitioners/providers must have an unencumbered license to participate in Blue Shield's provider network. The IPA/medical group must notify the Delegation Oversight Auditor of practitioners/providers that have been terminated via the HICE Report document and/or upon notification of the termination.

Appendix 4-A: Claims, Compliance Program, IT System Security, and Oversight Monitoring

Noted that this appendix applies to Delegated Entities and Specialty Health Plans.

Best Practices and Claims Adjudication

Audits and Audit Preparation

Updated section to indicate that a cover sheet is a required element in the claims audit and must be completed and attached to each claim sample.

Added the following language regarding required documents for audits:

If the contract cannot be submitted including the rate sheet specific to the claim, the Delegated Entity/Specialty Health Plan is required to demonstrate the payment methodology per claim in the audit webinar or submit claims system screen shots demonstrating how the claim was paid per contract or policy and procedure.

If the required documentation is not submitted and the Delegated Entity/Specialty Health Plan refuses to submit or review during the audit webinar, the audit will be closed as non-compliant (failed). The Delegated Entity/Specialty Health Plan will be reported to Blue Shield Contracting/Network Management for refusal to comply with audit requirements as outlined in provider contract and/or provider manual.

Updated in boldface type and strikethrough, the following regarding the timeframe for written results of audit deficiencies:

Blue Shield will provide the Delegated Entity**/Specialty Health Plan** with written results within ~~30 calendar~~ **10 business** days including an itemization of any deficiencies and whether or not the Delegated Entity**/Specialty Health Plan** must prepare and submit a formal, written corrective action plan to include root cause and remediation within ~~30 calendar~~ **10 business** days of receipt of audit results. If supporting documentation**/evidence is not provided the CAP will be closed as non-compliant.**

Corrective Action/Follow Up Audits

Deleted and ***replaced*** with the following:

Blue Shield performs, at a minimum, an annual claims and PDR audit. Follow-up audits will be scheduled by the assigned auditor if the Delegated Entity/Specialty Health Plan fails the annual audit. If applicable, as a result of a non-compliant follow-up audit, a remediation plan (Excel worksheet) will be requested from the Delegated Entity/Specialty Health Plan who must

submit by assigned due date from auditor. Based upon Blue Shield's tracking of remediation plan additional monitoring and/or remediation (follow up) validation audits will be performed. Based upon Blue Shield's tracking and outcome of the remediation plan, the Delegated Entity/Specialty Health Plan will be escalated to the Delegation Oversight Committee. This would include on-site visits, scheduled meetings, focal audits, and remediation project plan oversight.

For those Delegated Entities who are subject to DMHC audits, if deficiencies are determined during the review, a corrective action plan (CAP) is required to be sent to Blue Shield by the date provided by the Blue Shield and DMHC auditors. Additionally, Blue Shield may perform an unannounced audit dependent upon other indicators.

Compliance Program Effectiveness Oversight Audit

Added language indicating that Blue Shield utilizes CMS, DMHC, DHCS, OIG, DOI, and contractual requirements in its Compliance Program Effectiveness audit. Delegation Oversight will perform an annual audit of the effectiveness of your organization's Compliance Program as requested by CMS, DMHC and DHCS.

Added the following to the list of items the audit assessment includes:

- Evidence of database runs through the DHHS OIG List of Excluded Individuals and Entities (LEIE list), and the GSA Excluded Parties Lists System (EPLS) prior to the hiring or contracting of any new employee and provider
- Process for maintaining records for no less than ten (10) years – record retention
- Evidence of provider organization or limited Knox Keene oversight of sub-contractors (delegated)
    - Demonstrate oversight of all offshore and onshore sub-delegates (monitoring and annual audits) and approved and implemented policy and procedure for offshore sub-delegation

Added language detailing the process to submit a Corrective Action Plan (CAP). A CAP is required if found non-compliant with any audit element.

IT System Security

Deleted and ***replaced*** with the following:

Delegation Oversight will perform an IT system security and integrity audit to assure system access controls, policy and procedures regarding system changes, security of data, etc. are maintained. Oversight will also occur on security incident procedures and contingency plans for responding to an emergency or other occurrences that affect protection of Protective Health Information (PHI).

This audit is designed to perform oversight of delegated entities to ensure data is secure and cannot be manipulated or breached, and that the Delegated Entity/Specialty Health Plan has a process in place to address any fraudulent activities. Blue Shield is contractually required by all California and Federal Regulatory agencies and NCQA to conduct oversight of Delegated Entities IT systems and Disaster Recovery Plan/Strategy.

The oversight audit is also performed either via shared audit through HICE or individually on a biennial basis with possible quarterly monitoring. Please visit the HICE website for an

approved-evidence grid that is needed for submitting documentation as part of audit as well as policy and business rules to assist with understanding the audit history and requirements.

The Delegated Entity/Specialty Health Plan must submit documentation/evidence up to fifteen (15) business days of the request to BSCDOITSecurityAudit@blueshieldca.com.

The Delegated Entity/Specialty Health Plan is required to have specific personnel associated with the organization's IT systems involved in the audit.

Areas of overall concern to be reviewed include:

- Operational effectiveness
- Access to programs and data access rights role based
- Access to programs and data access control mechanisms and password complexity
- Program changes/standard change management
- Computer operations (backup, recovery, and resumption)
- HIPAA compliance and HIPAA technical safeguards
- Program changes including audit trails to identify data changes
- Access to programs and data access rights – internal controls and segregation of duty
- Access to IT privileged functions – monitoring of internal fraud and unauthorized overrides within IT system/applications

Oversight Monitoring

Added language to list of controls that Delegated entity should implement, in boldface type:

- Delegated Entity/Specialty Health Plan shall maintain a compliance program, and that the program is independent of fiscal and administrative management; **Delegated Entity/Specialty Health Plan shall provide a copy to Blue Shield**;
- **Delegated Entity/Specialty Health Plan shall maintain a disaster recovery plan and ensure that it is reviewed and/or updated annually. Delegated Entity/Specialty Health Plan shall provide a copy to Blue Shield.**

Blue Shield recommends the following IT Security Certification, HITRUST Risk-based r2 level certification. Secondarily, Blue Shield will accept SOC 2 Type II certification.

Added language detailing the process to submit a Corrective Action Plan (CAP). A CAP is required if deficiencies are identified.

Appendix 5-A: Utilization Management Delegation Standards

Added the following to the **UM Decision Timeframes – CMS Standards Table** which details UM requests, decision timeframes and notification timeframes:

- Part B and C Prescription Drugs
- Part D Prescription Drugs (only)

Appendix 5-B: Credentialing/Recredentialing Standards

Updated the standards to comply with NCQA requirements.