

Medicare Administrative Contractor (MAC) Provider Portal Handbook

Division of Provider Communications Technology

Provider Communications Group

May 2026

Version 4.1

Table of Contents

1	Introduction	5
1.1	... <i>About this Handbook</i>	5
1.2	... <i>Basic Portal Requirements</i>	5
1.2.1	Defining Portal Functions.....	5
1.3	... <i>MAC Transitions</i>	6
1.4	... <i>Portal Availability</i>	6
2	Enhancing, Redesigning, & Innovating a Provider Portal	6
3	Target Life Cycle (TLC)	6
4	CMS Technical Reference Architecture (TRA)	7
5	Security Requirements	7
5.1	... <i>Section 912 Evaluation</i>	7
5.1.1	Security Controls Assessment (SCA)	7
5.1.2	Authority to Operate (ATO).....	8
6	E-Authentication	8
6.1	... <i>Multi-factor Authentication</i>	8
6.2	... <i>Identity Management</i>	8
6.3	... <i>EDI for Authentication</i>	9
6.4	... <i>Recertification</i>	9
6.5	... <i>Authorization</i>	9
7	User Manual	9
8	Reporting.....	9
8.1	... <i>Provider Inquiries Evaluation System (PIES)</i>	9
8.2	... <i>PCSP Contractor Information Database (PCID)</i>	9
9	Appendices	10
9.1	... <i>CMS Portal Functions and Definitions</i>	10
9.2	... <i>CMS Detailed Functionality Descriptions</i>	12
9.2.1	Eligibility Inquiry	12
9.2.2	Claims-Related Transactions	13
9.2.3	Appeals Activities.....	13

9.2.4	Remittance Advice.....	13
9.2.5	Secure Messaging/Mailbox.....	14
10	Document Revisions	14

1 Introduction

1.1 About this Handbook

We prepared this handbook to support you as you develop, maintain, and enhance your MAC Internet-based portal. This handbook compiles best practices from our oversight of the portals.

Every portal is different. This handbook doesn't address all of the variations, activities, and processes for every portal, but it does provide the framework for a successful portal.

Work with your Contracting Officer Representative (COR) and the Division of Provider Communications Technology (DPCT) as you develop and enhance your portals.

1.2 Basic Portal Requirements

We encourage providers to use portals as a single system that allows them to access transactional content and services provided by multiple applications. Basic portal requirements include:

1. Minimum required functionality
2. [A user manual](#)
3. [Secure processes for access](#)
4. [Availability](#) 24 hours a day, 7 days a week, except for for normal claims processing, mainframe availability, and maintenance

1.2.1 Defining Portal Functions

Your portal must include **at least** the following functions:

- Claims Status
- Claims Submission (not applicable to DME or Part A)
- Eligibility Inquiry and Response
- MBI Lookup Tool
- Printable Entitlement Eligibility Page
- Remittance Advice
- Time Out Alerts
- Same or Similar (DME only)
- Appeals (Redeterminations, Reopenings and Part A Reconsiderations)

Other functions are at your discretion. Determine them based on provider needs, unless otherwise indicated by CMS. If you choose to add functionality that requires a new interface to another system or database, work with your COR and DPCT.

For more information:

- Appendix 9.1, [CMS Portal Functions and Definitions](#) (from the PCSP Contractor Information Database (PCID))

- Appendix 9.2, [CMS Detailed Functionality Descriptions](#) (includes IOM references for selected functionalities)

1.3 MAC Transitions

To minimize the impact on providers during a MAC transition, follow instructions for sharing portal information outlined in section [6.10 of the Medicare Administrative Contractor Workload Transition handbook](#).

1.4 Portal Availability

Although providers have the ability to speak to a Customer Service Representative (CSR) during normal Provider Contact Center (PCC) operating hours, automated “self-help” tools like the portals should be available for inquiries. Portals should be available 24 hours a day, 7 days a week with allowances for normal claims processing and system mainframe availability, as well as normal portal and system maintenance. When portals aren’t available, MACs should post a message on their website and the portal login page. For reporting, MACs should follow the guidance under [Portal Service Interruptions](#).

2 Enhancing, Redesigning, & Innovating a Provider Portal

You should continually update PCT on all portal activities including future enhancements to functionality, implementation dates, issues, and service interruptions.

Before redesigning your portal, you must get approval from your COR and DPCT. If you’re proposing enhancements that change Information Technology (IT) infrastructure, architecture, or the security boundary, submit your proposals according to TDL-250100 issued on 02/19/2025.

Your COR and DPCT will evaluate each portal redesign on a case by case basis.

3 Target Life Cycle (TLC)

The TLC is CMS's system development life cycle governance process. It promotes business flexibility and replaces point-in-time gate reviews with continuous evaluation and situational reviews. Work closely with your COR and DPCT throughout the TLC process.

Portals aren’t considered new systems; they’re modifications to the existing Internet architecture. Make sure you modify your existing documentation to include the portals, and let DPCT know when updated documentation is complete.

Alternate development methodologies, frameworks, and guidelines may be acceptable if they meet applicable federal legislative mandates (like FITARA and Clinger Cohen Act) and OMB/HHS policies.

[Get more information on the TLC.](#)

4 CMS Technical Reference Architecture (TRA)

The TRA provides CMS's authoritative technical architecture approach and technical reference standards to assure the secure and high-quality delivery of healthcare services to patients, providers, and business partners. The TRA is critical to effectively develop, transition to, and maintain CMS Processing Environments.

[Get more information on TRA.](#)

5 Security Requirements

Follow these requirements and standards for all of your portals:

- The Statement of Work
- [CMS Information Security & Privacy Contract Requirements](#)
- Security requirements in the current [IOM Pub 100-17, Section 5](#)

If you choose to redesign an existing portal or propose major enhancements (like adding claims submission functionality), we may require you to undergo a full or partial security control assessment and get a new Authorization to Operate (ATO) or update an existing ATO. In some cases, the portal may only need a partial security control assessment.

5.1 Section 912 Evaluation

The 912 Evaluation happens once your portal goes into production. During the evaluation:

- Work directly with the CMS Information System Security Officer (ISSO)
- Keep your CORs informed of the progress and results
- Make sure your portal meets 508 compliance requirements as outlined in Section H of your contract

5.1.1 Security Controls Assessment (SCA)

The Security Control Assessment (SCA), formerly known as a Security Test and Evaluation (ST&E), is a detailed evaluation of the controls protecting an information system. It determines the extent to which controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. See the [CMS Acceptable Risk Safeguards \(ARS\)](#)

Make sure you update pertinent information about the portal to ensure that you're effectively documenting security and privacy aspects of the portal. Load the updated documentation into CMS Federal Information Security Management Act (FISMA) Controls Tracking System (CFACTS). Those documents include:

- System Security Plan (SSP)
- Information Risk Assessment (IRA)

- Contingency Plan (CP)
- Privacy Impact Assessment (PIA)

5.1.2 Authority to Operate (ATO)

A system or application gets its ATO by performing System Certification and System Accreditation. The ATO provides Chief Information Officer (CIO) approval of System Certification and System Accreditation, authorizing the system to become operational. The ATO will be a modification of your overall ATO, rather than an ATO specific to the portal.

Once your portal has an ATO, it will be tested during regular Section 912 reviews and annual FISMA assessments to evaluate security controls.

6 E-Authentication

E-authentication is the process of establishing confidence in user identities presented electronically to an information system (see [OMB guidance OMB 04-04 and Revised guideline for electronic authentication of users](#)). Systems can use the authenticated identity to determine whether that individual is authorized to perform an electronic transaction.

E-authentication begins with registration. An applicant applies to a Registration Authority to become a subscriber of a Credential Service Provider (CSP). As a subscriber the applicant is issued or registers a token and a credential that binds the token to a name (and possibly other attributes) that the Registration Authority has verified. A token is something that the user possesses and controls (typically a key or password) and is used to authenticate the user's identity. The token and credential may be used in subsequent e-authentication events.

6.1 Multi-factor Authentication

Multi-factor authentication is required to access your portals. Under the CMS Information Security Requirements 1.2.2.6(H), you shall adhere to [CMS Acceptable Risk Safeguards \(ARS\)](#) and corresponding [Risk Management Handbook \(RMH\)](#), including those related to multifactor authentication.

We recommend the temporary MFA passcode be usable to each portal user for up to 12 hours. Direct any questions about multi-factor authentication to DPCT.

6.2 Identity Management

Identity Management assigns attributes to an identity and associates that identity to an individual. It includes the processes for maintaining and protecting identity data of an individual over the life cycle of the digital identity.

Identity Management can include, but may not be limited to:

- Using EDI Agreements to verify individuals who have permission to access provider data
- Using PECOS files to verify active enrollment relationships with their MACs

6.3 EDI for Authentication

Use data elements from your EDI agreements to authenticate providers, including clearinghouses and billing agencies. Consider a solution that enables you to further validate the relationship between the supplier and the third-party biller.

6.4 Recertification

Establish an annual recertification process for all portal users that includes each user ID and all of the National Provider Identifiers (NPIs) for which that ID has access.

6.5 Authorization

You're responsible for assuring that only authenticated portal users have the correct roles and authorities to access the various functionalities of the portal. This may include:

- Requiring providers to have a signed Electronic Data Interchange (EDI) Enrollment Agreement on file before granting access
- Establishing a written or electronic agreement with the primary portal administrators responsible for the registration/deactivation of users
- Verifying all administrators according to [CMS e-authentication requirements](#)

7 User Manual

You should develop a user manual which, at a minimum:

- Outlines registration, administrative, and security requirements
- Explains functionality

The user manual should be:

- Available electronically in the portal and on your provider education website
- Available in print upon request (if your portal doesn't allow users to print it)
- Updated and posted timely as portal functionalities change

Provide DPCT with a link to your user manual.

8 Reporting

8.1 Provider Inquiries Evaluation System (PIES)

By the 10th of each month, report the data elements specified in the PIES database related to your portal (the current [IOM Pub. 100-09, Chapter 6](#)).

8.2 PCSP Contractor Information Database (PCID)

By the 10th of each month, report portal functionality available in the previous month using the "Portal Functionality" module in PCID (the current [IOM Pub. 100-09, Chapter 6](#)).

Select from a list of functionalities found in Appendix 9.1, [CMS Portal Functions and Definitions](#).

If you're reporting on a functionality not listed, report it in the "Comments" box.

If you're reporting on planned functionalities, report it in the "Comments" box, and include the implementation periods.

8.2.1 Portal Service Interruptions

You're responsible for monitoring portal operations. You should take actions to quickly diagnose and correct issues and service interruptions (like unexpected downtime or unexpected availability of 1 or more functions).

When the portal isn't available:

- Post a message on your website and the portal login page
- Report portal service interruptions using the PCID Service Interruptions module (the current [IOM Pub. 100-09, Chapter 6](#))
- During portal status meetings, discuss with DPCT any service interruptions

9 Appendices

9.1 CMS Portal Functions and Definitions

Portal Functionality	Description
Audit and Reimbursement Document Submission	Capability to submit Audit and Reimbursement documentation.
Certificate of Medical Necessity (CMN) Detail (DME Only)	Capability to view CMN details (e.g., approved HCPCS and modifier, initial date, recertification/revision date, CMN status, CMN status date, length of need, last day item billed, total rental payments, and supplier information).
Claim Redetermination Status	Capability to check the status of a previously submitted Medicare redetermination.
Claim Redetermination Submission	Capability to submit a request for a Medicare redetermination.
Claim Reopening Status	Capability to check the status of a previously submitted reopening.
Claim Reopening Submission	Capability to submit a request for a Medicare reopening.
Claim Reconsideration Status	Capability to check the status of a previously submitted Medicare reconsideration.
Claim Reconsideration Submission	Capability to submit a request for a Medicare reconsideration.

Portal Functionality	Description
Claim Status	Capability to view the status/history of a single claim or range of claims submitted to the MAC.
Claim Submission	Capability to submit secure, electronic, HIPAA compliant claims.
Comparative Data Reports	Capability to generate/view/print a report that contains comparative data Medicare considers when determining how a provider's billing patterns contrast with other providers in the same specialty.
Educational Resources	Capability to link to educational resources, such as looking up procedure/diagnosis codes, forms, and billing information to assist providers with claim submission and research claim denials.
EFT Status	Capability to check the status of an EFT application.
Eligibility Inquiry and Response	Capability to submit an Eligibility Inquiry and view a beneficiary's Medicare eligibility data.
e-Pay/e-Check	Capability to remit payments (e.g., remitting offset demand overpayments) through the banking financial systems.
e-Offset	Capability to remit payments (e.g., remitting offset demand overpayments) internally through the MAC's Accounting department.
Financial Information	Capability to view financial summary information (e.g., recent checks issued, check number, issue date, check amount, check status, check cashed date, payment history, offset information, pricing, and Financial Control Numbers).
General Inquiry Submission	Capability to submit a question to a designated resource e-mailbox.
MBI Look-up Tool	Capability to search and view a beneficiary's Medicare Beneficiary Identifier (MBI).
Medical Review Information	Capability to submit information for clinical review of medical records to ensure that payment is made only for services that meet all Medicare coverage requirements and to also view Additional Documentation Requests (ADRs). (For further guidance, please see CR 10427.)
One-way Messaging	Capability to communicate one way: either MAC to provider or provider to MAC (no PII or PHI).
Overpayment Claims Adjustments	Capability to submit overpayment claim adjustment transactions.
Printable Entitlement Eligibility Page	Capability to print the eligibility data page.
Prior Authorization Request Status	Capability to view the status of a prior authorization request.

Portal Functionality	Description
Prior Authorization Request Submission	Capability to submit prior authorization requests.
Remittance Advice	Capability to view/print/download a remittance advice.
Same or Similar Eligibility (DME only)	Capability to check for same or similar equipment that has been issued to a beneficiary.
Secure two-way Messaging	Capability to send documents (sometimes with attachments) and/or inquiries and responses (including web chat capability) that contain PII or PHI two ways between the provider and the MAC.
Time Out Alerts	Capability to alert the user of the length of time remaining before the user would automatically be logged off the portal after a predefined period of inactivity.
View/Print Decision/Request Letters	Capability to view/print decision/request letters issued by the MAC (e.g., overpayment demand letters, audit results letters, and/or redetermination letters for ADS, ADR, MR, redeterminations, and appeals decisions).

9.2 CMS Detailed Functionality Descriptions

9.2.1 Eligibility Inquiry

[Checking Medicare eligibility](#) allows providers to confirm Medicare eligibility. You're required to use data from the HIPAA Eligibility Transaction System (HETS).

You must request a unique HETS submitter ID for each contract. Test all HETS releases to ensure that updates work with your portal. The HETS validation environment uses masked beneficiary data instead of real patient information and doesn't contain any production beneficiary records. You should only use the masked beneficiary data that is provided before each software release. Do not send eligibility requests using production beneficiary records as it will result in an error. [Get information about HETS and releases.](#)

Below are 3 options that providers may use to submit an eligibility inquiry:

Primary Search Option

- Subscriber¹ Last Name
- Subscriber First Name
- Subscriber Birth Date
- Subscriber Primary ID (MBI²)

¹ The subscriber is the patient (sometimes called a "beneficiary").

² The Medicare Beneficiary Identifier is the Medicare Number displayed on the Medicare Health Insurance card. We assign the MBI.

Alternate Search - Option 1

- Subscriber Last Name
- Subscriber Birth Date
- Subscriber Primary ID (MBI)

Alternate Search – Option 2

- Subscriber Last Name
- Subscriber First Name
- Subscriber Primary ID (MBI)

9.2.2 Claims-Related Transactions

Claims-related transactions require that the user submit key information about the patient or claim to get information. See the current [IOM 100-04, Chapter 24](#) for requirements.

[Claims status](#) functionality should give providers the ability to:

- View claims status
- Locate the status of a single claim or range of claims

Claims Submission functionality should:

- Give providers a secure platform enabling them to submit an electronic, HIPAA compliant claim
- Submit single claims, batch claims, or both

In accordance with the CMS Technical Reference Architecture (TRA), data must be saved in the data zone. It can't be saved in the presentation zone of the application.

9.2.3 Appeals Activities

When accepting appeal requests via the provider portal, follow the guidance issued in the current [IOM 100-04, Chapter 29](#).

9.2.4 Remittance Advice

A remittance advice (RA) is a notice of payments and adjustments sent to the entity submitting the claim (provider, supplier, or biller). An RA may serve as a companion to claim payments or as an explanation when there is no payment. The RA explains reimbursement decisions, including the reasons for payments and adjustments of processed claims.

CMS offers self-service tools for providers, including access to remittance information 24 hours/day, 7 days a week through the portals. The benefits of provider access to remittance information include:

- the ability to access remittances in order to track the timing of payments for faster communication and payment notification

- the ability to view information for a single claim in a remittance for faster account reconciliation
- the ability to view or print a remittance, as needed, saving on physical storage space

CMS wants to improve the provider experience with the availability of the remittance in the portal, and at the same time reduce costs. Suggestions for future enhancements include:

- Add a Help tab or mouse over functionality which includes clear descriptions of the Claim Adjustment Reason Codes and the Remittance Advice Remark Codes. This could also include a more descriptive explanation of why a payment has been adjusted.
- Reduce the number of paper remittances sent (including mailing costs) by discontinuing sending paper remittances to providers who currently have access the MAC provider portal.
- Further descriptive explanation of why a payment has been adjusted, such as Medicare specific explanations as displayed on Medicare Summary Notice (MSN).

9.2.5 Secure Messaging/Mailbox

Secure messaging offers providers a secure way to submit a request that can be responded to by the provider contact center or other business area of the MAC. This functionality may offer providers a way to complete forms and upload documentation as well as creates secure electronic, two-way communication between providers and MACs. The secure messaging may offer e-Form and application capabilities within the provider portal. Only authenticated users of the provider portal will be able to access this two-way communication.

10 Document Revisions

Date	Version Number	Document Changes
5/2026	4.1	Revisions to sections 1.2.1, 1.4, and 8 to reflect PCSP IOM changes and updated portal functions; Revisions to sections 2 – 6 to update hyperlinks; Revisions to section 9.1 to reflect current portal functions and definitions that align with PCSP modernization and reporting efforts; Revisions to section 9.2.1 to clarify information on HETS releases
4/2023	4.0	Revisions to section 2 to reflect TDL 190200; Revision to section 3 to update CMS processes for the Targeted Life Cycle which replaced the XLC; Revisions to section 4 to update information on the CMS technical reference architecture; Revisions to section 8 to include updated IOM references; Revisions throughout to make language clearer and more concise, updated and new hyperlinks, restructured for readability.

