Medicare Administrative Contractor (MAC) Provider Portal Handbook

Division of Provider Communications Technology

Provider Communications Group

June 2019

Version 3.2

Centers for Medicare & Medicaid Services

Document Revisions

Date	Version Number	Document Changes
05/24/2013	1.0	Initial Draft
10/22/2013	1.1	Revision based on initial comments received to CR 8491
01/21/2014	1.2	Revision to the "508 Compliance" section to reflect change to the process for existing portals. Rewording of text so that it is clear that the document is only meant to provide guidance
10/2016	2.0	Revision of handbook to reflect CMS intentions for portal maintenance, enhancements, and/or redesign; unavailability and service interruptions, project approvals, 912 audits, additional reporting requirements, portal functionality terms and descriptions, security requirements
8/2017	2.1	Revision to "E-Authentication" section to delete references to the e-authentication workbooks
11/2017	2.2	Revision to "Multi-factor Authentication" section to include link to Risk Management Handbook as well as a recommendation for "best practices" for the MFA one-time password
8/2018	3.0	Revision to Appendix 9.1 – update to portal functionalities and definitions
1/2019	3.1	Revision to Section 1.2 – update includes listing of minimum portal functionalities
6/2019	3.2	Revision to 6.1 "Multi-factor Authentication" to include an update to "best practices" for the MFA one-time password; revision to 9.2.2 to add language under claims submission functionality

Table of Contents

1 Introduction

1.1 Scope and Purpose

This handbook was prepared by CMS to provide strategic guidance in the form of high-level goals and guiding principles for quality, performance, and relationships among MAC Internet-based provider portals, herein referred to as "portals". This handbook represents a compilation of best practices, lessons learned and CMS experience in overseeing MAC portals. It is intended to generate awareness, discussion and support throughout all facets of portal strategy – specifically development, maintenance and enhancements. This handbook does not provide specific tactical guidance, but leaves such planning to the MACs, with Contracting Officer Representative (COR) approval and in cooperation with the Division of Provider Communications Technology (DPCT) in the Provider Communications Group (PCG)/Center for Medicare (CM). Your COR is the first line of contact for developing or enhancing a portal. Your COR will provide you with the PCG liaison.

Every portal will vary depending on the unique circumstances and environment of the MAC involved. There may be activities and processes described in this handbook that will not be applicable to a specific portal. There may also be activities that will need to be performed that the handbook does not cover. The handbook cannot identify and address all of the variations that may occur within the development, maintenance, or enhancement of a portal nor all of the tasks for which a MAC will be responsible. However, it will provide the framework for a successful portal and guidance in addressing situations as they arise.

MACs should maintain collaborative and cooperative efforts with their COR as well as DPCT/PCG throughout all aspects of portal development and enhancement.

1.2 Basic MAC Responsibilities

Providers are encouraged to use self-service portals. Through a MAC's portal, a provider should gain access to transactional content and services provided by multiple applications. The provider should perceive the multiple applications as one system since the portal should implement common mechanisms for navigation, e-authentication and layout for all content and services.

The portal should be offered to access various healthcare transactions. At a minimum portal functions should include, but not be limited to the following:

- Claims Status
- Eligibility Inquiry and Response
- MBI Lookup Tool
- Printable Entitlement Eligibility Page
- Remittance Advice

- Time Out Alerts
- Same or Similar (DME only)

A comprehensive list of portal functions and reporting requirements are outlined in sections 7 and 8 of this handbook.

MACs must provide a portal user manual to providers. The user manual should be available electronically and posted on the contractor's provider education website. The user manual may be printed and distributed upon request from the provider if the MAC does not have the functionality to allow the provider to print it. As provider portal functionality changes, the user manual should be updated timely and the revisions posted to the provider education website.

MACs should have a secure process in place for granting user access to the portal, which may include, but not be limited to requiring providers to have a signed Electronic Data Interchange (EDI) Enrollment Agreement on file before granting access to the portal. MACs should have a written or electronic agreement in place with the primary portal administrators who are responsible for the registration/deactivation of users at their facility. MACs should ensure that all administrators have been verified in accordance with the CMS e-authentication requirements.

1.3 MAC Transitions

In order to minimize the impact on the provider community during a MAC transition, certain outgoing MAC portal information shall be shared with the incoming MAC. MACs shall follow instructions for sharing portal information outlined in section 6.10 of the Medicare Administrative Contractor Workload Transition handbook located at: http://www.cms.gov/Medicare/Medicare-Contracting/Medicare-Administrative-Contractors/Downloads/A-B-DME-Workload-Transition-Handbook-June-2014.pdf

1.4 Portal Availability

Although the provider shall have the ability to speak to a Customer Service Representative during normal Provider Contact Center (PCC) operating hours, automated "self-help" tools, such as the portals should also be used by all MACs to assist with handling inquiries. As such, the portal should be available to providers 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 information is not available, MACs should post a message alerting providers on the MAC website and the portal login page. MACs should follow the guidance under section 8.2.1, Portal Service Interruptions for reporting purposes.

2 Redesigning and Enhancing a Provider Portal

CMS does not require notification of routine portal maintenance. However, should a MAC choose to redesign and/or make major enhancements to an existing portal, approval must first be obtained from the MAC's COR in coordination with the PCG liaison. A major enhancement is defined as one where the change will result in a new portal interface with another system or database, such as adding claims processing functionality to the portal or significant changes to the portal such as security posture changes.

2.1 Approval Process

When a MAC determines the necessity for either redesigning or enhancing their portal, the MAC should develop a proposal which clearly outlines:

- Portal functionality
- Objectives
- Cost
- Timeframes
- States involved
- Number and types of providers
- Type of contract
- e-authentication process
- Success criteria
- Methods for accessing eligibility, claims data and other data sources for functionality for the proposed application
- Security Impact Analysis (SIA)

The proposal should also include details about similar private-side applications and three-zone architecture. The COR and PCG liaison will be responsible for reviewing the proposal and making a determination on how to proceed.

Once approval for a redesign or enhancement is obtained, each portal redesign will be evaluated on a case by case basis by MCMG and PCG regarding the next steps. If deemed necessary, as part of the XLC process, processes may include developing architectural compliance, coordinating efforts with the Technical Review Board (TRB), providing artifact templates for XLC process phases, etc.

3 Expedited Lifecycle Process (XLC)

3.1 XLC General Description

The XLC model provides a streamlined approach to project oversight and execution. It is the next generation of project life cycle processes with a flexible approach to project

execution and governance where the level of governance is directly associated with the complexity of the project. This model promotes agility, effective review of projects, and determines appropriate oversight early in the process – increasing predictability and efficiency.

For additional information regarding the XLC process, see http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/XLC/index.html

3.2 MAC Responsibilities for the XLC Process

MAC provider portals are considered modifications to the existing Internet architecture and are not considered new systems. As such, existing MAC documentation should be modified to include the provider portals. The MAC must ensure that all documentation has been modified and must notify the PCG liaison when that has occurred.

The MAC will be responsible for the following:

- Making initial contact with the PCG liaison after receiving COR approval
- Presenting ideas for the provider portal including portal development, functionality and enhancements with the PCG liaison
- Developing the artifacts specified in the Project Process Agreement (PPA)
- Working with the PCG liaison on any draft TRB templates (including TRB consult, preliminary design review and/or detail design review) prior to a scheduled meeting with the TRB

NOTE: The MAC should ensure the COR is updated on their progress after every gate review of the XLC process. The MAC should work with their COR to determine the best methods for receiving updates.

3.3 Project Process Agreement (PPA)

A customized PPA for provider portals has been approved. The PPA authorizes and documents the justifications for using, not using, or combining specific reviews and the selection of specific work products. The project's complexity will determine which artifacts are needed for a project—as documented in the Project Process Agreement (PPA). You may view the PPA at http://www.cms.gov/Medicare/Medicare-Contracting/FFSProvCustSvcGen/Downloads/Project-Process-Agreement-for-Internet-portals.zip.

The phases of the XLC that the MAC must complete and the artifacts that are required will be indicated in the Project Process Agreement.

3.4 Requirements Analysis and Design

During the Requirements Analysis and Design Phase, a common set of business rules are refined and the business requirements are validated and decomposed into functional and non-functional requirements. The requirements are used to define the design in detail, including inputs, processes, outputs, and interfaces, and permit further detailed project management planning. Detailed specifications are developed to support the IT solution that fulfills the requirements for a particular release. The requirements and logical description of the entities, relationships, and attributes of the data are defined and allocated into system and data design specifications. Initial traceability is started between requirements, design and solution testing. These design specifications are organized in a way suitable for implementation and testing within the constraints of a physical environment (e.g., computer, database, and infrastructure).

3.4.1 XLC Governance Reviews

During requirements analysis and design, the MAC will meet, in conjunction with the PCG liaison, with the Technical Review Board (TRB). The TRB is involved in the XLC governance reviews.

NOTE: The PCG liaison is the primary point of contact between the MAC and the TRB. In this role, the PCG liaison will schedule any/all meetings with the TRB to discuss provider portals.

At a minimum, when redesigning or enhancing a portal, MACs may be asked to prepare presentations for the following TRB meetings and/or gate reviews:

- TRB Consult
- Preliminary Design Review (PDR)
- Detailed Design Review (DDR)

The purpose and content for each of these gate reviews is discussed in section 3.4.3, Content for Governance Reviews:

3.4.2 Process for TRB Meetings:

Depending on the complexity of the proposed changes/enhancements to the portal, the TRB process/timeframes may change. Adding additional functionality or making enhancements to the portal may require less TRB involvement than redesigning the portal. Below is an outline which describes the general process for meeting with the TRB and basic timeframe guidelines.

1. Send PCG liaison proposal which details the portal development or enhancement:
    a) PCG will review initial proposal within 2 weeks of receipt

b) PCG will determine the type of TRB meeting necessary (consult, PDR, DDR)
c) PCG will work with TRB and MAC to schedule meeting a minimum of 3 months after discussing the proposal with the MAC. Timeframe will be determined by proposal complexity (Scheduling is driven by the TRB and their availability)

2. PCG will provide the MAC with the appropriate TRB presentation template to be used during the meeting
    a) The MAC will have 1 month (date to be specified by PCG) to complete the appropriate TRB presentation template
    b) The MAC will submit the draft presentation template to PCG for comments
    c) PCG will provide comments and schedule follow-up meetings with the MAC as necessary within 2 weeks

3. The MAC will submit the final TRB presentation to PCG no later than 1 week prior to the scheduled TRB meeting
    a. The MAC will have 1 month (date to be specified by PCG) to complete the appropriate TRB presentation template
        i. If the final presentation is not submitted by the MAC within the given timeframe, PCG may choose to cancel the TRB meeting
        ii. The TRB requires PCG to send an electronic version of the presentation and any additional diagrams no later than 1 week prior to any TRB meeting

3.4.3 Content for Governance Reviews:

Content for each TRB meeting will vary slightly depending on the type of governance review the PCG liaison deems appropriate.

1. TRB Consult
    a. The consult is an informal discussion with the TRB to gain a broader perspective as well as ensure alignment with the enterprise architecture. The main goal is for the MAC to present plans for either redesigning or enhancing the portal and obtain TRB recommendations and/or opinions. No decisions from the TRB will be made during the consults.
    b. The MAC should have specific, focused questions on what feedback is needed from CMS before proceeding. The TRB will provide the MAC with advice and help steer the MAC in the appropriate direction for any proposed portal changes.
2. PDR and/or DDR
    a. The PDR and DDR are formal discussions with the TRB in which the MAC will present detailed information on any proposed changes to the portal at both the preliminary and final designs, respectively.

b. The MAC should include a visual representation of the System Architecture and how the portal will interact with other systems. Visual representations should enhance the TRB presentation slides and should include, but not be limited to the following:
    i. Indicate present-day portal architecture from redesigned and/or enhanced portal architecture
    ii. How to trace data in and out of the system
    iii. How the data is moved, modified and stored
    iv. Lines that indicate connections - the users and what path(s) they are using to access the application
    v. Every server involved and how it is configured
    vi. Security configuration changes, if any
    vii. Depict the FISS, MCS and VMS systems to show how the portal is receiving "real time status checks" against those
    viii. Where the SSL is being terminated
c. The MAC should incorporate into any provider portal planning the efforts undertaken to achieve data modeling.

The MAC has the option of whether they would like to attend the TRB in-person or over the phone. If the MAC decides to attend it over the phone, they may contact their PCG liaison and ask the liaison to print and supply the color copies of the presentation at the TRB meeting. Visio files cannot be printed at CMS – MACs should send pdf files of any diagrams to be printed. When the MAC attends the TRB in-person, the MAC should print out color copies of the final TRB presentation and provide them to the TRB members during the meeting.

3.5 Development and Test

During the Development and Test Phase, the detailed requirements and design information documented in the Requirements Analysis and Design phase will be transformed into machine-executable form. The detailed requirements and design information will be verified and validated so that all of the individual system components (and data) of the IT solution function correctly and interface properly with other components within the system. Test data and test case specifications will be finalized, and tests will be conducted for individual components, integration, and end-to-end functionality from end-consumer to all systems and back, testing all federal and state agencies, as appropriate, to ensure accurate functionality and data.

If a MAC chooses to host its provider portal development/test at its MAC site and not the EDC, the MAC will be required to establish a logically isolated staging environment on non-production virtual LANs (VLANs) within the confines of the production multi-zone network. The VLANs are a network of computers that behave as if they are connected to a single,

network segment even though they may actually be physically located on different segments of a LAN. This solution would provide the ability to test redundancy, failover, and have all components, including F5 LTMs, for final system integration and configuration tests.

The following reviews mentioned correspond to phases of the life cycle and are performed to ensure that exit criteria for any given phase has been covered. The PCG liaison and TRB will advise the MAC as to which reviews are necessary for their individual portals.

3.5.1 Validation Readiness Review (VRR)

The purpose of the VRR is to ensure the system/application completed thorough Development Testing and is ready for turnover to the formal, controlled test environment for Validation testing.

3.5.2 Implementation Readiness Review (IRR)

The purpose of the IRR is to ensure that the information technology (IT) solution or automated system/application that has been developed is ready for implementation activities, such that the required system hardware, networking and telecommunications equipment; COTS, GOTS, and/or custom-developed software; and database(s) can be installed and configured in the test and/or production environments.

3.5.3 Production Readiness Review (PRR)

The purpose of the PRR is to ensure that the infrastructure contractor's operational staff has the appropriate startup and shutdown scripts, accurate application architecture documentation, application validation procedures, and valid contact information to ensure operability of infrastructure applications.

3.5.4 Operational Readiness Review (ORR)

The purpose of the ORR is to ensure the system/application completed its implementation processes according to plan and that it is ready for turnover to the Operations & Maintenance team and operational release into the Production environment.

3.6 Pre-Implementation

Prior to moving into production, the application will need to go through a Security Control Assessment (SCA) to obtain an Authority to Operate (ATO). Detailed information on both the SCA and ATO are found in Section 5, Security Requirements of this handbook

3.7 Implementation

During the Implementation Phase, the IT solution will be put into production based on the MAC's modified Authority to Operate (ATO). The MACs will work with MCMG and the PCG liaison to develop the appropriate implementation timeline that falls in line with the MACs' annual 912 audit.

3.8 Operations & Maintenance

After implementation, the IT solution will enter the Operations & Maintenance (O&M) Phase. In O&M the IT solution system components, data, and infrastructure will be maintained in the production environment and monitored to ensure they continue meeting business needs.

3.8.1 Post Implementation Review (PIR)

The purpose of the PIR is to review project performance to evaluate: Customer Satisfaction, Strategic and Business Results, Financial Performance, and Innovation. The PIR is the first Annual Operational Analysis (AOA) and is conducted 6 – 9 months after implementation.

3.8.2 Annual Operational Analysis (AOA)

The purpose of the AOA is to evaluate system performance, user satisfaction with the system, adaptability to changing business needs, and new technologies that might improve the system. This review is diagnostic in nature and can lead to development or maintenance activities. Ultimately, the AOA determines whether the IT investment should continue, be modified, or be terminated.

3.8.3 Disposition Review (DR)

The purpose of the DR is to ensure that the IT investment has been completely and appropriately transitioned and disposed, thereby ending the life cycle of the IT project. A Disposition Closeout Certificate is issued upon successful completion of this review.

4 CMS Technical Reference Architecture (TRA)

Any MAC provider portal will be required to be developed and maintained using CMS-approved architectural, security and database standards for a three-zone Internet architecture application to extend to providers within its jurisdiction for inbound and outbound transactions.

The CMS TRA, and its associated supplements, documents the standard architecture for all of the CMS production environments. The supplements document specific technical solutions in support of the TRA.

The following is a list of the documents available. Not all of the documents listed will be relevant to MAC provider portals. The MAC and the PCG liaison will determine which documents are needed based on its portal design. If the MACs should have any questions determining which documents are needed, they are to work with their PCG Liaison. The MAC should request the TRA documents from the PCG liaison once its high-level proposal is approved, ensuring that its architecture meets the CMS requirements. Before making any

modifications to the application, the MAC should check with the PCG liaison to make sure that it is in possession of the most current versions of the TRA documents.

4.1 Foundation Document and Governance Supplements

- Technical Reference Architecture
- Architecture Change Request (ACR) Process
- Architecture Change Request Form (ACR)
- TRB Business Rules

4.2 TRA Supplements (in alphabetical order)

- Access Control and Identity Management
- Application Performance Monitoring
- Business Intelligence
- Customer Relationship Management
- Data Archiving Services
- Distributed Systems Platform Supplement
- Domain Name System Services
- Enterprise Content Management
- Enterprise File Transfer
- Enterprise Storage Architecture and Storage Services
- Internet Protocol version 6 (IPv6)
- NET Application Development Guidelines
- Java EE Application Development Guidelines
- Open Source Software
- Portal Strategy
- Security Services Supplement
- Shared Services
- Technology Products Portfolio
- Virtualization
- WAN Services Supplement
- Web Services

4.3 Technology Products Portfolio

The set of approved software products at CMS are defined by this supplement

- Technology Products Portfolio
- Technology Products Portfolio – Approved Products List

5 Security Requirements

The MAC will be required to conduct all security administration activities for all parts of the Internet-facing applications within its jurisdiction in accordance with all requirements and standards identified in the SOW and outlined at the following website:

http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/index.html?redirect=/InformationSecurity/15_Procedures.asp

The MAC should follow security requirements outlined in IOM Pub 100-17, section 5 as well as meet the CMS Security requirements listed at: https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html .

When a MAC chooses to redesign an existing portal or proposes major enhancements such as adding claims submission functionality, MACs will be required to undergo a full or partial security control assessment and obtain a new ATO or update an existing ATO for the portal. A partial security control assessment will be used to cover those changes associated with a significant system change.

5.1 Section 912 Audit

Once the portals have an ATO, they will be tested during the Section 912 audits in subsequent years. The purpose of the annual FISMA assessment is to evaluate security controls associated with the system.

The 912 audit for the provider portal will occur after the portal has gone into production. At that point, the MAC will work directly with the Centers for Medicare Information System Security Officer throughout the audit process. The MAC should keep its COR informed of its progress with the audit.

As part of the 912 audit, the MAC portals will be evaluated on their 508 compliance. The MACs should work with the CMS ISSO to ensure requirements for 508 are met. MACs shall follow the 508 requirements outlined in Section H of their contract.

5.1.1 Security Controls Assessment (SCA)

The SCA, formerly known as a Security Test and Evaluation (ST&E), is a detailed evaluation of the controls protecting an information system. The security control assessment 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. Requirements for control assessments are described in the CMS Acceptable Risk Safeguards (ARS) in the Security Assessment and Authorization (CA) section of the document.

Each document from the MAC's initial security audit should be modified to include pertinent information regarding the provider portals. Once the documents are modified, the MAC should load them into CMS Federal Information Security Management Act (FISMA) Controls Tracking System (CFACTS). Those documents include:

- System Security Plan
- Information Risk Assessment

- Contingency Plan
- Privacy Impact Assessment (PIA)

5.1.2 Authority to Operate (ATO)

A system/application obtains its ATO by virtue of performing System Certification and System Accreditation. The ATO provides CIO approval of System Certification and System Accreditation, authorizing the system to become operational. The ATO will be a modification of the MACs overall ATO rather than one specific to the portal.

6 E-Authentication

In accordance with OMB guidance [OMB 04-04], e-authentication is the process of establishing confidence in user identities presented electronically to an information system. 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) and, as a subscriber, 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

Effective June 26, 2015, CMS requires contractors with network access to CMS systems to use two-factor authentication to access such systems. Under the CMS Information Security Requirements 1.2.2.6(H), MACs shall adhere to the CMS Acceptable Risk Safeguards (ARS) and corresponding Risk Management Handbooks (RMH), including those related to multifactor authentication at https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/RMH_VIII_4-3_Non-Std_Acct_Auth_Mgmt.pdf. As a best practice, CMS recommends that the temporary "one-time password" be available to portal users for up to 12 hours. MACs shall direct any questions or concerns regarding two-factor authentication to the PCG Liaison.

6.2 Identity Management

The primary goal of Identity Management is to establish a trustworthy process for assigning attributes to an identity and to associate that identity to an individual. Identity management includes the processes for maintaining and protecting the 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 the PECOS files for verification of active enrollment relationships with their MACs

6.3 EDI for Authentication

Ideally, data elements from MAC EDI agreements should be used for purposes of authenticating providers, including clearing houses and billing agencies, into the portals. Ideally, MACs should consider a solution that would enable them to further validate the relationship between the supplier and the third party biller.

6.4 Recertification

MACs should establish an annual recertification process for all portal users. This recertification process should include each user ID, as well as all of the NPIs for which that ID has access.

6.5 Authorization

The MAC is responsible for assuring that authenticated portal users only have the correct roles and authorities to access the various functionalities of the MAC portal application.

7 Portal Functionality

A MAC should develop a user's manual, accessible to providers, which, at a minimum, outlines the portal's registration requirements, functionality and administrative and security requirements for accessing the portal. This user's manual should be available to those logged into the portal as well as accessible from the MAC's website to those who may not have access to the portal. The user's manual should also be provided to the PCG liaison.

7.1 Defining Portal Functions

A MAC should determine its provider portal's functionality based on the needs of its providers and pending COR and PCG liaison approval. Functionalities will be at the discretion of each MAC. When a MAC chooses to add functionality that requires a new interface to another system or database, such as with claims submission, the MAC will coordinate efforts through the XLC process with their PCG liaison.

Appendix 9.1, CMS Portal Functions and Definitions provides a table of the CMS defined portal functionalities as found in the PCSP Contractor Information Database (PCID). Appendix 9.2, CMS Detailed Functionality Descriptions provides some detailed descriptions and IOM references for selected functionalities.

8 Reporting

8.1 Provider Inquiries Evaluation System (PIES)

CMS collects and displays provider contact center performance data on a monthly basis. For MACs, this data is collected through PIES at https://www.pie-system.com. MACs are required to report the data outlined in the PIES user manual. For a list of MAC provider portal fields and their definitions, please see the PIES Definitions and PIES User Guide documents contained in the PIES system at https://www.pie-system.com/documentation.asp.

8.2 PCSP Contractor Information Database (PCID)

CMS has developed a new module in PCID named "Portal Functionality." MACs are required by CR 9682, issued on 10/7/2016, to report in the "Portal Functionality" module their current Portal Functionalities (section 70.2.3.9 of IOM Pub. 100-09, Chapter 6). MACs are to select from a CMS specified list of functionalities which can be found in Appendix 9.1, CMS Portal Functions and Definitions . If the MAC has a portal functionality currently not listed, the MAC is required to report that functionality in the "Comments" text box provided in the module. MACs are also required to report in the "Comments" text box any known future planned portal functionalities and their implementation period(s). MACs are required to report portal functionality by the 10th of the month for portal functionality available in the previous month and, if applicable, report future portal functionality in accordance with the data entry screens in the Portal Functionality module.

8.2.1 Portal Service Interruptions

MACs are responsible for monitoring their portal operations and shall take the necessary action to quickly diagnose and correct any issues impacting their ability to provide portal service to providers. MACs are required by CR 9682, issued on 10/7/2016, to report Internet-based provider portal service interruptions (unexpected portal downtimes and/or loss of one or more portal functions that cause the portal or function(s) to be unavailable to providers) in PCID (section 70.2.3.8 of IOM Pub. 100-09, Chapter 6). MACs shall report these portal interruptions by the 10th of the month for portal interruptions occurring in the previous month in the Telecommunications Service Interruptions data entry screen in PCID. MACs are also required by CR 9682 to send a Contractor Alert to CMS at the time of an unexpected portal downtime or the unexpected unavailability of a portal function(s) that creates an adverse effect on the MAC's Provider Contact Center (section 30 of IOM Pub. 100-09, Chapter 6).

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 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.

Portal Functionality	Description
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.
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. This functionality may include the 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, ADRs, MR, redeterminations, and appeals decisions).
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.

Portal Functionality	Description
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

The eligibility verification process will allow providers to quickly and easily confirm Medicare eligibility for beneficiaries. Such inquiries will be required to use the HIPAA Eligibility Transaction System (HETS) as the source of the eligibility information. Each contract that the MAC has must request a unique HETS submitter ID. Because HETS uses the ASC X12 270-271 transactions, a MAC should test all HETS releases to ensure that its portal functionality is not negatively affected by updates. Information about HETS and releases to the application is posted to the CMS website at https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/HETSHelp/index.html

There are three options which may be used to submit an eligibility inquiry:

Primary Search Option

- Subscriber[1] Last Name
- Subscriber First Name
- Subscriber Birth Date
- Subscriber Primary ID (HICN[2])

[1] The subscriber is the patient. The patient is also referred to as a beneficiary by Medicare.

[2] The Health Insurance Claim Number (HICN) is the Medicare beneficiary identifier assigned by Medicare. When looking at the Medicare Health Insurance card, the HICN is the Medicare Claim Number displayed on the card.

Alternate Search - Option 1

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

Alternate Search – Option 2

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

9.2.2 Claims-Related Transactions

Claims-related transactions require that the user submits key information about the beneficiary and/or claim in order to get response information. See IOM 100-09, Chapter 6, Section 80 located at http://www.cms.gov/Regulations-and-Guidance/Guidance/Manuals/Downloads/com109c06.pdf for data requirements.

Claims Status functionality should:

- Give providers the ability to view claims status,
- Give providers the ability to locate the status of a single claim or range of claims submitted to Medicare

Claims Submission functionality should:

- Give providers a secure platform enabling them to submit an electronic, HIPAA compliant claim,
- If a MAC decides to provide claims submission they may either do single claims (currently claims submission in existing provider portals is done through individual submissions), Batch Claims, or both.
- A critical design element for claims submission is the configuration of data entry of the claim. MACs should note that, In Accordance With (IAW) the CMS Technical Reference Architecture (TRA), data cannot be saved in the presentation zone of the application; it must be saved in the data zone.

9.2.3 Appeals Activities

When accepting appeal requests via the provider portal, MACs will be required to follow the guidance issued in IOM 100-04, Chapter 29, Section 310 located at http://www.cms.gov/Regulations-and-Guidance/Guidance/Manuals/Downloads/clm104c29.pdf.

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 a claim payment(s) or as an explanation when there is no payment. The RA explains the 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 displaced 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 eForm and application capabilities within the provider portal. Only authenticated users of the provider portal will be able to access this two-way communication.

As CMS explores better ways to simplify mechanisms for business functions that require a secure way to transmit information such as prepayment review, prior authorization, and postpayment review, a robust secure messaging functionality in the portal will be of increasing importance.