HMSA'S VENDOR QUICK GUIDE TO COMPLIANCE

2025

HMSA's Vendor Quick Guide to Compliance

Introduction

The purpose of this document is to guide HMSA vendors in the development and maintenance of an effective compliance program.

While a compliance program is important for all vendors, this quick guide focuses on those that perform services required by HMSA's contracts with regulators, including Centers for Medicare & Medicaid Services (CMS), Office of Personnel Management – Office of the Inspector General, and the Hawaii Department of Human Services Med-QUEST Division. These vendors have different names depending on the line of business:

Line of Business	Vendor Classification
Medicare	First Tier, Downstream, and Related entities (FDRs)
Medicaid	Subcontractors
Affordable Care Act	Delegated entities
Federal Plan 87 and Federal Employee Plan (FEP)	Subcontractors

This quick guide may use any of the above terms and the general terms *vendor* and *you/your*.

NOTE: If you are unsure if the quick guide applies to you, please reach out to your HMSA vendor contact.

Why is this quick guide important?

HMSA is required by regulators to maintain an effective compliance program; therefore, HMSA holds our vendors to the same compliance program requirements. This guide is an educational tool regarding requirements and recommendations.

The information focuses on various compliance areas and is based on seven elements of an effective compliance program:

1. Written policies, procedures, and standards of conduct.
2. Compliance officer, compliance committee, and high-level oversight.
3. Effective training and education.
4. Effective lines of communication.
5. Well-publicized disciplinary standards.
6. Effective system for routine monitoring, auditing, and identification of compliance risks.
7. Procedures and system for prompt response to detected compliance issues and undertaking corrective action.

Prevention, Detection, and Correction Framework

The key aspects of an effective compliance program can be broken into prevention, detection, or correction controls. Throughout this guide, we'll outline which elements correlate to each of the three controls.

- Prevention: These controls provide a framework to operate, communicate compliance expectations, and prevent repeated issues from recurring.
- Detection: These controls indicate opportunities for improvement within the compliance program. Detection controls may include monitoring and detecting compliance issues.
- Correction: These controls allow for immediate and reasonable responses to misconduct and compliance violations. Correction controls may include escalation processes and corrective action plans.

Examples of delegated functions

Delegated entities can perform various functions related to administrative or health care services.

Some examples include:

- Sales and marketing.
- Utilization management.
- Quality improvement.
- Applications processing.
- Enrollment, disenrollment, and membership functions.
- Claims administration, processing, and coverage adjudication.
- Appeals and grievances.
- Licensing and credentialing.
- Pharmacy benefit management.
- Hotline operations.
- Customer service.
- Bid preparation.
- Outbound enrollment verification.
- Provider network management.
- Processing of pharmacy claims at the point of sale.
- Negotiation with prescription drug manufacturers and others for rebates, discounts, or other price concessions on prescription drugs.
- Administration and tracking of enrollees' drug benefits, including TrOOP balance processing.
- Coordination with other benefit programs such as Medicaid, state pharmaceutical assistance, or other insurance programs.
- Entities that generate claims data.
- Health care services.

If the services you perform for HMSA are not listed above, you may still be a delegated entity and should check with your HMSA vendor contact on whether this quick guide applies to you.

Elements of effective compliance

Policies and procedures

Policies act as a guide for employees in understanding corporate expectations, methods of reporting, and relevant contact information. It's imperative to maintain compliance policies to demonstrate the establishment and communication of an organization's compliance expectations. HMSA provides you with a copy of its Code of Conduct to provide clarity about the HMSA's internal standards and expectations, and it's available at https://www.hmsa.com/content/assets/code-of-business-conduct.pdf.

You should also have written policies and procedures that address the following:

- Standards of conduct: A set of ethical and compliance-related expectations for employees to follow. This should be provided to your employees and other applicable individuals and entities within 90 days of hire, upon update, and annually thereafter.
- Organization's commitment to comply with federal and state laws, regulations, rules, and other requirements.
- Training requirements and time frames.
- Methods of communicating and reporting issues: Outline the expectation to report compliance concerns and suspected or actual violations, including the reporting of compliance issues to HMSA.
- An environment of non-intimidation and non-retaliation for good faith reporting.
- Disciplinary standards.
- Identification of corporate compliance leadership, especially the corporate compliance officer.
- Record retention practices.

Policies and procedures generally fall under prevention controls, and HMSA may request copies of standards of conduct and other compliance policies, proof of annual review, and proof of distribution, according to the terms of your HMSA contract.

Compliance structure

- Maintaining the necessary compliance structure and reporting relationships may help demonstrate that you have appropriate oversight of your compliance program. It illustrates leadership is invested in the effectiveness of the compliance program independent of operational goals. It's recommended that you maintain the following structure. **(Prevention control)**

Basic structural building blocks

Compliance officer	• Employee. • Direct reporting to senior-most leader and governing body. • Meet with the compliance committee quarterly. • Independent involvement with compliance program.
Compliance committee	• Meet at least quarterly. • Review compliance issues.
Governing body	• Annual approval of the standards of conduct. • Reasonable oversight of the effectiveness of the compliance program.

You can demonstrate evidence of your compliance structure in many ways and may include:

- Organization charts illustrating reporting lines.
- Meeting minutes and agendas documenting participants, items discussed, and decisions made as they relate to the compliance program.
- Committee charters.
- Communications about the compliance officer, including contact information.

Training

Vendors must complete general compliance and fraud, waste, and abuse (FWA) training. Your employees and other eligible individuals must take the training within 90 days of hire or start date and at least annually thereafter. **(Prevention control)**

- Provide your own compliance training to your employees and verify your applicable subcontracted entities are doing the same.
- Complete HMSA's FWA training.
- Incorporate CMS content of the standardized training modules from the website into your own training materials.

Vendors are also encouraged to provide supplemental training. Examples may include reporting protocols, conflict of interest, the Health Insurance Portability and Accountability Act, HITECH, and the Anti-Kickback law.

Wait! Does everyone have to take the training?

Vendors should consider the roles and responsibilities of staff to determine who is required to take the training. Generally, individuals who should complete the training include:

- Senior administrators or managers directly responsible for the contract with the plan sponsor.
- Individuals directly involved with establishing and administering the plan sponsor's formulary and/or medical benefits.

- Individuals involved with decision-making authority on behalf of the plan sponsor.
- Reviewers of beneficiary claims and services submitted for payment.
- Individuals with job functions that place the vendor in a position to commit significant noncompliance with CMS program requirements or health care FWA.

Evidence of training can be presented in many ways and may include:

- Sign-in sheets.
- Completion certificates.
- Attestations confirming completion of the CMS training.
- Copy of training material.
- List of training dates, hire dates, and cycle of annual training.
- Governing body completion of training.
- Record retention demonstrating attendance, topics, and scores.

Communication and issue tracking

Vendors must maintain lines of communication to provide their employees and subcontracted entities with important regulatory information, compliance information, reporting protocols, and issue tracking expectations. The lines of communication should be accessible to all, allow the reporting of compliance and FWA issues, and allow anonymous and confidential good faith reporting of issues. The method of accessing and utilizing these lines of communication should be publicized throughout the facility and be user-friendly and available 24 hours a day. (Prevention control)

Keeping lines of communication open demonstrates an active effort to keep everyone informed of necessary information and allows for the reporting of issues.

Maintaining a system to receive, record, respond to, and track compliance questions or reports of suspected or detected noncompliance or potential FWA is also important. HMSA and vendors must educate employees about identifying and reporting potential FWA. If the vendor experiences any issue of noncompliance, FWA, or breach, it's imperative they notify HMSA appropriately. (Detection control) Your HMSA vendor contact should track any issues reported, actions taken or planned to be taken to remediate those issues, when the item was considered closed, and how the vendor plans to prevent the same issue from occurring. (Correction control)

Evidence of communication and issue-tracking can be presented in many ways and may include:

- Availability of lines of communication, including physical postings, email, intranet, meeting minutes, and training.
- Communications about regulatory changes, impact, and action items.
- Reporting procedures.

- Policy language: Outline reporting and investigation protocol or options for anonymous reporting.
- Issues tracking log.
- Dashboard or scorecard to track corrective actions.

Disciplinary standards

Vendors should have disciplinary standards that address and correct instances of employee misconduct. The standards should identify noncompliance, illegal, or unethical behavior. Employees should understand the consequences of participating in noncompliant or FWA-related activities. There should be an emphasis on maintaining an environment for non-retaliation for good faith participation in the compliance program. The disciplinary standards should outline different stages of reprimand, up to and including termination.

It's important to demonstrate strong publication of these disciplinary standards. Evidence of training can be presented in many ways and may include:

- Methods of publication, including newsletters, staff meeting minutes, compliance training, and intranet.
- Policy language outlining the above,

Monitoring, auditing, and identifying compliance risks

Regulators hold HMSA wholly accountable for the work our vendors perform as if HMSA is performing the work ourselves. As HMSA is responsible for establishing and implementing an effective system for routine monitoring, auditing, and identifying compliance risks, HMSA requires the same of vendors.

The system should include both monitoring and auditing activities, which are defined below. These activities are aimed at protecting against noncompliance and potential FWA, as well as monitoring compliance with regulatory guidance, federal and state laws, and internal policies and procedures. **(Detection control)**

Monitoring	Regular reviews performed as part of normal operations to confirm ongoing compliance and ensure that corrective actions are undertaken and effective.
Auditing	Formal review of compliance with a particular set of standards used as base measure.

Monitoring activities are usually conducted within the business areas or the people involved with the day-to-day work. Auditing activities are usually conducted by an independent unit within the business or an external party.

How to assign scope for the monitoring and auditing activities?

Identifying compliance risks that occur throughout the year will help determine what type of activities should be performed. Once the risks are identified, you should have a plan to address the identified risks. Risks should also be ranked by priority, which should be revised as new risks are added. Ideally, you would focus on addressing the highest risks first. Monitoring and auditing activities are often the answer to addressing these risks. (Detection control)

Exclusion screening

Individuals and entities that are excluded from participating in federal programs must not perform work or render services on these programs. Screening for excluded individuals and entities is done by checking against the HHS Office of the Inspector General List of Excluded Individuals and Entities (LEIE), System for Award Management (SAM), and the Office of Personnel Management – Office of the Inspector General exclusion lists. Furthermore, the Hawaii Department of Human Services excludes individuals and entities that are listed on the LEIE or the State's Provider Exclusion Reinstatement List from providing services in the Medicaid program.

The purpose of checking these lists is to avoid paying any federal or state funds to individuals, providers, or entities that are listed on any of these exclusion lists. Vendors who contract with HMSA are required to check these lists and provide evidence that these checks were completed. These exclusion lists should be reviewed prior to hiring or contracting and monthly thereafter for:

- Employees.
- Contractors.
- Temporary employees.
- Owners, agents, and managing employees.
- Consultants.
- Governing body members.
- Major shareholders (5% or more.
- Volunteers.

(Detection control)

Evidence may include:

- List of all applicable employees and entities (or number of individuals and entities) with dates checked, results of the checks, and actions taken to resolve any positive indications.

- Routine informal audits by the contract administrator to verify the vendor's process is accurate.

Medicare preclusion screening

Vendors that process Medicare claims are required to maintain a preclusion process. Your vendor manager will send the preclusion list to you monthly, and your processes must include the following activities:

- Remove the precluded vendors from your network.
- Provide a report to HMSA of members with dates of service with the precluded provider that fall within 12 months of the date the provider was added to the Preclusion List.
- Deny any future Medicare request for payments as of the preclusion effective date.

HMSA may request copies of your preclusion processes and/or may review claims payments to ensure payments are not made to precluded providers.

Privacy and Security

Protecting our member data

We are often required to share our members' information with our vendors. However, before HMSA can provide this information to a vendor, federal privacy and security regulations (under the Health Insurance Portability and Accountability Act) require that vendors sign a contractual agreement called a Business Associate Agreement (BAA). The BAA makes sure that a vendor has certain safeguards in place to protect member information.

The information that requires safeguards falls into two categories, Personally Identifiable Information (PII) and Protected Health Information (PHI).

What are some examples of PHI or PII?

Personally Identifiable Information (PII) is any information that alone, or in combination with other information, identifies or could reasonably identify an individual or their relatives, employers, or household members.

Protected Health Information (PHI) is any information created or received that identifies an individual or for which there is a reasonable basis to believe it can be used to identify an individual, relating to the:

- Past, present, or future physical or mental health condition of an individual.
- Provision of health care to an individual.
- Past, present, or future payment for the provision of health care to an individual.

Examples of PHI and PII include an individual's:

- Name.
- Address.
- Date of birth or age.
- Telephone number.
- Fax number.
- Email address.
- Social Security number.
- Health plan ID or subscriber number.
- Medical account number.
- Medical contract number.
- Medical claim number.
- Diagnosis code.
- Medical procedure code.
- Dates of medical service.
- Genetic information.
- Certificate/license number.
- Medical device identifier and serial number.

- Internet address.
- Internet protocol address number.
- Vehicle identifier and serial number, including license plate numbers.
- Full face photographic image and any comparable images.
- Any other unique identifying number, characteristic, or code.

The company strives to protect all PHI and PII. Any unauthorized disclosure of PHI or PII should be reported to HMSA as described in your contract.

As a matter of practicality, we recommend you extend the safeguards used for PHI and PII to an individual's financial information as well.

What is a privacy incident?

An unauthorized use of HMSA's PII or PHI within your organization or

An unauthorized disclosure of HMSA's PII or PHI to an unauthorized or unintended third-party recipient.

What is a security incident?

Any event affecting information systems that results in a compromise to the confidentiality, integrity, or availability of HMSA's information.

What to do when there is a privacy or security incident:

If there is an incident that impacts HMSA's information, you're required to report the incident to HMSA as soon as possible, but no later than the time frame indicated in your contract. Please follow the procedure for reporting incidents as described in your contract. The report should include as much information about the event known at the time of reporting, and to the extent known, including:

- Date and time the event occurred.
- Date the event was discovered.
- Complete description of the PII or PHI accessed, used, or disclosed.
- Complete description of the event, including the cause, and the names and the effect on the systems or data involved.
- Contact information for communications regarding the event.
- Initial mitigating action taken to contain the event and an assessment of the level of compromise to HMSA's data.
- Plan to correct the compromises to HMSA's data and to prevent future occurrences.

Blue Cross Blue Shield Association License Standard

HMSA is an independent licensee of the Blue Cross Blue Shield Association (BCBSA). BCBSA makes protection of PHI and PII a priority under the Blue Cross Blue Shield Association's License Standards.

BCBSA plans exercise reasonable and appropriate oversight of their Business Associate's data security controls used to safeguard and protect the plan's PHI and PII. To comply with BCBSA standards and with federal privacy and security laws, BCBSA plans require that all Business Associates have an up-to-date, signed BAA. It's HMSA's responsibility to ensure compliance with these requirements. HMSA takes compliance seriously and it's the responsibility of our vendor partners to assist in helping us maintain it.

Section 508 compliance

HMSA is a recipient of federal funds and therefore must be compliant with Section 508 of the United States Workforce Rehabilitation Act of 1973. Section 508 mandates that all electronic and information technology developed, procured, maintained, or used by the federal government be accessible to people with disabilities.

As a vendor, you will be doing work on behalf of HMSA and therefore must also follow section 508. As an entity that receives federal funding, CMS requires that you be compliant with Section 508 as well. CMS has made available resources for assistance in creating 508 compliant documentation. Please visit https://www.section508.gov/ and https://www.cms.gov/cms-section-508-tools-resources to learn more.

Record retention

Vendors must retain records related to their compliance programs, including training and screening. These records must be retained for a period of 10 years, unless otherwise specified in the Business Associate Agreement.

Code of business conduct

What is it?

Conducting our business with integrity in accordance with industry standards and all applicable laws, regulations, and mandates is required and expected. The Code of Business Conduct is a critical document that provides workforce members with the framework for decision-making. Together, these elements serve as a compass that empowers workforce members to "do the right thing" by adhering to ethical business conduct standards. The Code of Business Conduct ties all the above stated components together and is the driving factor behind our recommended practices.

How does it apply to vendors?

Vendors aren't exempt from the above stated ethical expectations. Our vendors are held to the same code of conduct as our employees. Compliance and Ethics assists vendor managers in ensuring vendors are meeting ethical standards.

How to report an ethical issue:

Vendors and their staff can report potential issues to the toll-free compliance hotline at 1 (800) 749-4672. This is an anonymous, confidential hotline available 24 hours a day, seven days a week. Don't wait to report or allow for issues of ethical compliance to grow. Report the issue as soon as possible to our direct lines of communication.

Strengthening vendor relationships with compliance partnerships

In the constantly evolving world of health care compliance, it's important to stay current on government regulations. HMSA is committed to assisting our vendor partners in meeting regulatory requirements and the provisions of the Health Insurance Portability and Accountability Act as business associates.