



Compassion. Excellence. Integrity.

STAFF AI TRAINING

Education, Competency
and Safe AI Use in
Home Health Care

COMMITTED TO SAFE AND
RESPONSIBLE USE OF ARTIFICIAL
INTELLIGENCE TO ENHANCE
PATIENT CARE AND OUTCOMES



SAFE USE

Using AI safely
and responsibly
in all aspects of
patient care.



PROTECT PRIVACY

Safeguarding
patient information
in compliance with
HIPAA and agency
policies.



ENSURE QUALITY

Maintaining accurate
documentation,
clinical judgment,
and high standards
of care.



BUILD COMPETENCY

Providing education
and practical tools
to confidently
and effectively use
AI technologies.



PUT PATIENTS FIRST

AI supports our
mission—compassionate,
personalized, and
patient-centered care.

INNOVATION. INTEGRITY. COMPASSION.

TOGETHER, WE USE TECHNOLOGY TO ENRICH CARE,
EMPOWER STAFF, AND IMPROVE LIVES.

TABLE OF CONTENTS ARTIFICIAL INTELLIGENCE (AI) USE POLICY i

PART I — ARTIFICIAL INTELLIGENCE STAFF EDUCATION & COMPETENCY

1	Introduction to Artificial Intelligence	1
2	AI Fundamentals	1
3	AI in Home Health	2
4	Human Oversight	2
5	Professional Responsibilities	2
6	Documentation Integrity	2
7	HIPAA & Privacy	2
8	CMS Conditions of Participation (CoPs)	3
9	Ethical AI	3
10	Cybersecurity	3
11	Fraud, Waste & Abuse	3
12	Documentation Standards	3
13	AI Hallucinations	3
14	Clinical Decision Support	3
15	Case Studies	3

PART II — GUIDED NOTES, EXERCISES & CASE SCENARIOS

A	Guided Notes	4
B	Practical Exercises	4
C	Exercise: Identifying Appropriate & Inappropriate AI Use	5
D	Human Oversight Reminder & Practice Activity	6
E	Discussion Questions	6
F	Documentation Exercise	9
1	Scenario 1 – Skilled Nursing Visit	10
2	Scenario 2 – Home Health Aide Visit	12
3	Scenario 3 – Physical Therapy Visit	13
4	Scenario 4 – Medication Review	14
G	Documentation Review Checklist & Group Discussion	15

TABLE OF CONTENTS

ENHANCED TOPICS — EXPANDED SUBJECT REFERENCE

1	AI Governance	21	16	Incident Investigations	37
2	AI Ethics	21	17	Root Cause Analysis	39
3	Documentation Integrity (Expanded)	22	18	Vendor Management	41
4	Clinical Reasoning	23	19	Data Ownership	44
5	Human Oversight (Expanded)	24	20	Explainable AI	46
6	AI Limitations	25	21	Bias Mitigation	47
7	AI Hallucinations (Expanded)	26	22	Patient Communication	49
8	Documentation Cloning	27	23	AI-Assisted Voice Documentation	51
9	Copy-and-Paste Risks	28	24	Remote Work Security	53
10	Upcoding and Downcoding	29	25	Secure Mobile Device Use	56
11	False Claims Act	30	26	AI in Interdisciplinary Care	58
12	OIG Fraud Examples	31	27	Disaster Recovery	60
13	Medicare Documentation Expectations	32	28	Business Continuity	63
14	Surveyor Red Flags	34	29	AI Performance Monitoring	66
15	QAPI Monitoring	35	30	Competency Validation	69
A	Knowledge Checks	72			
B	Final Examination	72			

FORMS & COMPETENCIES

1	AI Risk Assessment Tool	74	8	AI Clinical Validation Checklist	86
2	AI Vendor Evaluation Checklist	77	9	AI Incident Report Form	88
3	AI Security Assessment Checklist	79	10	AI Privacy Breach Report Form	90
4	AI Implementation Readiness Checklist	81	11	AI Annual Competency Checklist	92
5	AI User Access Authorization Form	83	12	AI Quarterly Audit Tool	94
6	AI Disclosure and Patient Acknowledgment	84	13	AI QAPI Monitoring Dashboard	96
7	AI Documentation Review Checklist	85	14	AI Corrective Action Plan (CAP)	98

USE OF ARTIFICIAL INTELLIGENCE (AI)

Policy and Procedure

PURPOSE

The purpose of this policy is to establish comprehensive standards governing the acquisition, implementation, oversight, monitoring, security, and responsible use of Artificial Intelligence (AI) technologies within the Home Health Agency. This policy establishes a governance framework that promotes the safe, ethical, and compliant use of AI while protecting patient safety, clinical integrity, documentation accuracy, patient privacy, and regulatory compliance.

The Agency recognizes that Artificial Intelligence has the potential to improve operational efficiency, support clinical documentation, enhance quality improvement activities, strengthen regulatory compliance, improve staff education, and assist workforce members with administrative and operational tasks. However, Artificial Intelligence is intended solely to function as an assistive technology and shall never replace the independent clinical judgment, professional responsibilities, ethical obligations, licensure, or accountability of qualified healthcare professionals.

This policy establishes minimum standards to ensure Artificial Intelligence technologies are implemented in a manner that:

- Promotes safe, high-quality patient care.
- Protects patient rights and confidentiality.
- Supports accurate, individualized, and complete clinical documentation.
- Maintains compliance with all applicable federal and state laws and regulations.
- Preserves the integrity of the medical record.
- Prevents fraud, waste, and abuse.
- Ensures meaningful human oversight of all AI-assisted activities.
- Supports continuous quality improvement and risk management.

The Agency is committed to ensuring that Artificial Intelligence enhances—not replaces—the knowledge, experience, critical thinking, and professional judgment of licensed healthcare professionals.

POLICY STATEMENT

It is the policy of the Home Health Agency that Artificial Intelligence may be utilized only as an assistive tool to support administrative, educational, operational, quality improvement, and clinical documentation activities when such use complies with Agency policies, the Health Insurance Portability and Accountability Act (HIPAA), the CMS Conditions of Participation (CoPs), applicable state laws, accreditation standards, and all other applicable federal and state regulations.

Artificial Intelligence shall never independently perform patient care functions or replace the clinical decision-making responsibilities of licensed healthcare professionals. AI-generated information shall always be considered advisory in nature and shall require meaningful human review, verification, modification when appropriate, and final approval by the responsible workforce member before implementation or incorporation into any Agency record.

All workforce members remain personally and professionally responsible for every document, assessment, recommendation, communication, coding decision, clinical decision, and patient care activity that is created, reviewed, edited, approved, or authenticated with the assistance of Artificial Intelligence.

The Agency shall implement appropriate governance, education, cybersecurity safeguards, quality monitoring, and oversight processes to ensure Artificial Intelligence technologies are used safely, ethically, and in accordance with accepted professional standards.

The Agency further recognizes that the use of Artificial Intelligence is continually evolving. Accordingly, this policy shall be periodically reviewed and updated to address new technologies, regulatory requirements, accreditation standards, cybersecurity risks, and emerging best practices.

SCOPE

This policy applies to all workforce members, regardless of employment status or work location, who access, utilize, supervise, develop, manage, or otherwise interact with Artificial Intelligence technologies on behalf of the Agency.

This policy applies to, but is not limited to:

- Governing Body Members
- Agency Administrator
- Director of Nursing (DON)
- Alternate Director of Nursing
- Clinical Manager(s)
- Registered Nurses (RNs)
- Licensed Practical Nurses (LPNs), where applicable
- Physical Therapists (PTs)
- Occupational Therapists (OTs)
- Speech-Language Pathologists (SLPs)
- Medical Social Workers (MSWs)
- Home Health Aides (HHAs)
- Medical Records Personnel
- Quality Assessment and Performance Improvement (QAPI) personnel
- Coding and OASIS Review Staff
- Billing Personnel
- Human Resources Personnel
- Information Technology Personnel
- Privacy Officer
- Security Officer
- Contractors
- Consultants
- Temporary Personnel
- Any other individual authorized to perform work on behalf of the Agency.

This policy applies to all Agency-owned, Agency-licensed, Agency-approved, or Agency-authorized Artificial Intelligence technologies used for:

- Administrative support
- Clinical documentation assistance
- Educational content
- Staff competency development
- Patient education
- Operational workflow improvement
- Quality improvement activities
- Coding assistance
- OASIS review assistance
- Regulatory research
- Data analytics
- Reporting

- Communication support
- Risk management activities

This policy applies regardless of whether Artificial Intelligence is accessed through desktop computers, laptops, mobile devices, cloud-based applications, integrated Electronic Medical Record (EMR) systems, voice recognition software, or other approved technologies.

GUIDING PRINCIPLES

The Agency adopts the following guiding principles for the responsible use of Artificial Intelligence throughout the organization.

A. Patient Safety

Patient safety shall remain the Agency's highest priority. Artificial Intelligence shall never compromise patient safety or replace appropriate clinical assessment, observation, or professional judgment.

B. Human Oversight

Meaningful human oversight shall be maintained for every use of Artificial Intelligence involving patient care, clinical documentation, quality activities, coding, communications, or decision support. No AI-generated output shall be accepted without independent human review and approval.

C. Professional Accountability

Artificial Intelligence does not assume legal, ethical, or professional responsibility for patient care. Every licensed healthcare professional remains individually accountable for the accuracy, completeness, appropriateness, and authenticity of all patient care services and documentation.

D. Documentation Integrity

Clinical documentation shall accurately reflect services actually provided, observations personally obtained, and professional clinical judgment exercised by the responsible clinician. Artificial Intelligence shall never create, fabricate, exaggerate, omit, or misrepresent patient information.

E. Privacy and Confidentiality

The Agency shall protect Protected Health Information (PHI) through appropriate administrative, physical, and technical safeguards. Patient information shall only be entered into Agency-approved Artificial Intelligence systems that meet applicable privacy and security requirements.

F. Ethical Use

Artificial Intelligence shall be used honestly, ethically, transparently, and responsibly. AI shall never be used to deceive patients, misrepresent clinical services, manipulate documentation, or obtain improper reimbursement.

G. Regulatory Compliance

All AI activities shall comply with applicable federal and state laws, CMS Conditions of Participation, HIPAA, accreditation standards, Agency policies, and accepted professional standards of practice.

H. Continuous Improvement

The Agency shall continually evaluate Artificial Intelligence technologies to improve patient care, operational effectiveness, cybersecurity, documentation quality, and regulatory compliance while identifying and mitigating associated risks.

DEFINITIONS

For purposes of this policy, the following definitions apply:

Artificial Intelligence (AI): Computer systems or software capable of performing tasks that normally require human intelligence, including generating text, analyzing information, recognizing patterns, assisting with documentation, producing recommendations, or supporting decision-making.

Generative Artificial Intelligence (Generative AI): A category of AI capable of producing original content such as written text, summaries, reports, educational materials, images, or other information based on user prompts.

Machine Learning: A branch of Artificial Intelligence that enables computer systems to improve performance by identifying patterns within data without being explicitly programmed for every task.

Clinical Decision Support (CDS): Technology that provides clinicians with evidence-based recommendations or relevant clinical information intended to support—but never replace—professional clinical judgment.

Artificial Intelligence Hallucination: Information generated by an AI system that appears credible but is false, fabricated, inaccurate, incomplete, misleading, or unsupported by factual evidence.

Human Oversight: The independent review, verification, evaluation, modification as necessary, approval, and authentication of AI-generated information by an appropriately qualified workforce member before such information is relied upon or incorporated into the patient's legal medical record.

Protected Health Information (PHI): Individually identifiable health information protected under the Health Insurance Portability and Accountability Act (HIPAA).

Meaningful Human Review: A thorough evaluation performed by a qualified workforce member to confirm that AI-generated information is accurate, patient-specific, clinically appropriate, complete, and consistent with applicable laws, regulations, physician orders, and professional standards.

Authentication: The process by which an authorized workforce member confirms the accuracy and completeness of documentation through signature or other approved authentication method, thereby accepting professional responsibility for the content.

Approved AI System: An Artificial Intelligence application that has been evaluated, approved, and authorized by the Agency for use in accordance with Agency policies and applicable regulatory requirements.

Prompt: Instructions or information entered into an AI system to generate a response or output.

Bias: A systematic error within an AI system that may result in inaccurate, unfair, or discriminatory recommendations or outputs.

Risk Assessment: A formal evaluation conducted to identify, analyze, and mitigate risks associated with implementing or using Artificial Intelligence technologies.

Business Associate Agreement (BAA): A written agreement required under HIPAA when a vendor creates, receives, maintains, or transmits Protected Health Information on behalf of the Agency.

Cybersecurity Incident: Any actual or suspected event involving unauthorized access, disclosure, alteration, destruction, ransomware, malware, phishing, data loss, or compromise of information systems.

Workforce Member: Employees, contractors, volunteers, students, consultants, temporary personnel, and any other individual performing work under the direction or control of the Agency.

GOVERNANCE AND OVERSIGHT

The Agency shall establish and maintain an Artificial Intelligence governance program to ensure AI technologies are implemented, monitored, and used safely, ethically, securely, and in compliance with applicable laws and regulations.

Oversight of the Agency's Artificial Intelligence Program shall be provided by the Governing Body through delegated authority to the Administrator, Privacy Officer, Security Officer, Director of Nursing, Clinical Leadership, and the Artificial Intelligence Oversight Committee.

The AI Oversight Committee shall include representatives from administration, clinical services, quality improvement, information technology, privacy and security, medical records, and other departments as appropriate. The Committee may also include consultants or subject matter experts when necessary.

The AI Oversight Committee shall be responsible for:

- Reviewing and approving proposed AI technologies prior to implementation.
- Evaluating risks associated with AI applications.
- Ensuring compliance with applicable laws, regulations, accreditation standards, and Agency policies.
- Monitoring documentation quality and patient safety related to AI use.
- Reviewing AI-related incidents, privacy concerns, and cybersecurity events.
- Recommending corrective actions when deficiencies are identified.
- Monitoring performance indicators through the Agency's Quality Assessment and Performance Improvement (QAPI) Program.
- Evaluating staff competency and training needs.
- Reviewing vendor performance.
- Recommending policy revisions based on regulatory changes, emerging technologies, or identified risks.
- Reporting significant findings and recommendations to the Governing Body.

The Governing Body retains ultimate responsibility for oversight of the Agency's Artificial Intelligence Program and shall ensure adequate resources are available to maintain compliance with this policy.

APPROVED AI SYSTEMS

Only Artificial Intelligence technologies that have been formally reviewed and approved by the Agency may be used to perform Agency business or process Agency information.

Prior to implementation, each proposed AI system shall undergo a documented evaluation that includes, at a minimum:

- Functional and operational review.
- Clinical appropriateness review, when applicable.
- Privacy and HIPAA compliance review.
- Information security assessment.
- Cybersecurity risk assessment.
- Vendor evaluation.
- Review of data ownership and retention practices.
- Verification of encryption and access controls.
- Determination of Business Associate Agreement (BAA) requirements.
- Assessment of regulatory compliance.
- Evaluation of integration with existing Agency systems.
- User training requirements.
- Implementation approval by designated Agency leadership.

Only Agency-approved AI systems may be used to create, review, edit, summarize, analyze, or process Agency information, including Protected Health Information.

Workforce members are prohibited from entering Agency business information, patient information, Protected Health Information, confidential Agency documents, or other sensitive information into public, consumer-grade, or otherwise unauthorized Artificial Intelligence applications.

The Agency reserves the right to restrict, suspend, or discontinue the use of any Artificial Intelligence technology when concerns arise regarding patient safety, privacy, cybersecurity, regulatory compliance, vendor performance, or documentation integrity.

The Agency shall maintain an inventory of approved Artificial Intelligence technologies and periodically reevaluate each system to ensure continued compliance with applicable legal, regulatory, operational, and security requirements.

APPROVED USES OF ARTIFICIAL INTELLIGENCE (AI)

The Agency authorizes the use of Artificial Intelligence (AI) solely as a support tool to improve efficiency, enhance documentation quality, assist workforce members with administrative and operational activities, and promote quality patient care. AI shall be used only within the limits established by this policy and only through Agency-approved AI systems.

All AI-generated content shall be independently reviewed, verified, modified as necessary, and approved by the responsible workforce member before implementation, distribution, or incorporation into the patient's legal medical record.

The use of AI shall never diminish the professional responsibilities, ethical obligations, clinical judgment, or accountability of licensed healthcare professionals.

A. Administrative Support

Artificial Intelligence may be used to assist with administrative functions including, but not limited to:

- Drafting Agency policies, procedures, and forms.
- Preparing letters, memoranda, reports, and correspondence.
- Developing meeting agendas and meeting summaries.
- Assisting with scheduling and operational planning.
- Creating quality improvement reports.
- Assisting with human resources documentation.
- Developing educational presentations.
- Organizing administrative information.
- Preparing committee reports.
- Supporting business planning activities.

Administrative documents generated with AI shall be reviewed for accuracy, completeness, consistency with Agency operations, and regulatory compliance before implementation.

B. Clinical Documentation Support

Artificial Intelligence may assist clinicians in improving the organization, clarity, readability, and efficiency of clinical documentation.

Examples include:

- Improving grammar, spelling, and punctuation.
- Organizing narrative documentation.
- Formatting visit notes.
- Summarizing clinician-written documentation.
- Assisting with professional wording.
- Identifying incomplete documentation for clinician review.
- Assisting with development of patient education materials.
- Organizing interdisciplinary communication.
- Preparing documentation templates.

AI may assist with documentation formatting but shall never replace the clinician's own assessment, observations, clinical reasoning, or professional judgment.

C. Education and Training

Artificial Intelligence may be used to support workforce education by assisting with:

- Development of orientation materials.
- Annual competency education.
- Continuing education materials.
- Skills validation tools.
- Knowledge assessments.
- Clinical case studies.

- Mock survey preparation.
- Patient education materials.
- Caregiver educational resources.

Educational materials containing clinical information shall be reviewed and approved by qualified clinical personnel prior to distribution.

D. Quality Assessment and Performance Improvement (QAPI)

Artificial Intelligence may assist with quality improvement activities including:

- Trend analysis.
- Outcome analysis.
- Performance dashboards.
- Regulatory compliance monitoring.
- Clinical audit support.
- Documentation review assistance.
- Identification of quality improvement opportunities.
- Statistical reporting.
- Risk identification.
- Performance indicator monitoring.

Quality reports generated using AI shall always be validated by designated quality personnel prior to implementation or presentation.

E. Regulatory and Research Support

Artificial Intelligence may assist workforce members in locating publicly available regulatory guidance, professional standards, clinical practice recommendations, and educational resources to improve Agency compliance and patient care.

AI-generated regulatory summaries shall not replace independent review of official regulatory publications when required.

F. Coding Assistance

Artificial Intelligence may provide coding support by assisting qualified personnel with:

- ICD-10 coding suggestions.
- OASIS review assistance.
- Identification of documentation inconsistencies.
- Coding research.
- Clinical terminology clarification.

Artificial Intelligence shall not independently determine diagnoses, assign reimbursement codes, or replace the judgment of qualified coding professionals.

G. Operational Improvement

Artificial Intelligence may be used to support Agency operations by assisting with:

- Workflow analysis.
- Process improvement.
- Operational planning.
- Resource utilization.
- Productivity analysis.
- Data organization.
- Communication efficiency.
- Business analytics.

Operational recommendations shall be reviewed by Agency leadership prior to implementation.

PROHIBITED USES OF ARTIFICIAL INTELLIGENCE (AI)

Artificial Intelligence shall never be used in any manner that compromises patient safety, documentation integrity, professional accountability, ethical practice, or regulatory compliance. The following activities are strictly prohibited.

A. Independent Clinical Decision-Making

Artificial Intelligence shall never independently:

- Diagnose medical conditions.
- Establish or modify a Plan of Care.
- Determine medical necessity.
- Prescribe medications.
- Recommend medication changes without clinician review.
- Replace physician clinical judgment.
- Replace licensed clinician judgment.
- Determine patient eligibility for services.
- Establish visit frequencies.
- Determine discharge readiness.
- Independently make patient care decisions.

B. Clinical Assessments

Artificial Intelligence shall never:

- Perform patient assessments.
- Replace comprehensive assessments.
- Complete comprehensive assessments.
- Replace OASIS data collection.
- Independently complete OASIS assessments.
- Replace medication reconciliation.
- Replace pain assessments.
- Replace fall risk assessments.
- Replace wound assessments.
- Replace clinician observations made during a home visit.

C. Documentation Creation Without Verification

Artificial Intelligence shall never be used to:

- Generate documentation for visits not performed.
- Create documentation without clinician review.
- Create false documentation.
- Fabricate assessment findings.
- Fabricate patient statements.
- Fabricate caregiver education.
- Fabricate interventions.
- Fabricate physician communications.
- Fabricate medication information.
- Fabricate vital signs.
- Fabricate wound measurements.
- Fabricate functional status.
- Create documentation for another clinician.
- Create documentation for future visits.
- Modify documentation to improve reimbursement.

D. Fraud, Waste, and Abuse

Artificial Intelligence shall never be used to:

- Uppcode diagnoses.
- Downcode services.
- Increase reimbursement inappropriately.
- Misrepresent services provided.
- Alter documentation after the fact to justify billing.
- Produce duplicate documentation between patients.
- Copy documentation from one patient to another.
- Create cloned documentation.
- Create fraudulent medical records.
- Conceal documentation deficiencies.
- Misrepresent clinician findings.

E. Authentication

Artificial Intelligence shall never:

- Sign documentation.
- Authenticate documentation.
- Electronically sign clinical records.
- Replace clinician signatures.
- Replace physician authentication.
- Replace required supervisory visits.
- Replace interdisciplinary conferences.
- Replace required patient contacts.

F. Privacy and Security

Artificial Intelligence shall never be used to:

- Enter Protected Health Information into unauthorized AI applications.
- Upload confidential Agency documents into public AI systems.
- Circumvent cybersecurity safeguards.
- Share confidential information with unauthorized individuals.
- Store Agency data in unauthorized systems.

Violation of these prohibitions may result in disciplinary action, termination of employment or contractual relationship, suspension of AI privileges, mandatory retraining, reporting to regulatory agencies or professional licensing boards when required, and other corrective actions deemed appropriate by the Agency.

HUMAN OVERSIGHT AND PROFESSIONAL ACCOUNTABILITY

Artificial Intelligence is intended solely to assist workforce members in performing administrative, operational, educational, quality improvement, and documentation-related activities. Artificial Intelligence does not replace human judgment, professional reasoning, ethical responsibilities, or clinical accountability.

Meaningful human oversight is mandatory for every use of Artificial Intelligence involving Agency operations, patient care, or clinical documentation.

The responsible workforce member shall independently review every AI-generated output prior to its use, implementation, communication, distribution, or inclusion within the patient's legal medical record.

The review shall include verification of:

- Patient identity.
- Date of service.

- Assessment findings.
- Physician orders.
- Medication reconciliation.
- Clinical observations.
- Vital signs.
- Functional assessments.
- Wound assessments.
- Interventions provided.
- Patient response to treatment.
- Caregiver education.
- Goals of care.
- Plan of Care consistency.
- Clinical reasoning.
- Narrative accuracy.
- Coding accuracy.
- Regulatory compliance.

If inaccuracies, omissions, inconsistencies, hallucinations, or unsupported statements are identified, the workforce member shall immediately correct or remove the AI-generated information before it is finalized.

Artificial Intelligence recommendations shall always be considered advisory. Final clinical decisions shall be made solely by qualified healthcare professionals exercising independent clinical judgment. Each workforce member remains personally responsible for all documentation authenticated under their name regardless of whether Artificial Intelligence assisted in preparing the document.

No workforce member may rely upon Artificial Intelligence as a substitute for:

- Professional education.
- Clinical competency.
- Patient assessment.
- Ethical decision-making.
- Independent judgment.
- Professional accountability.

The use of Artificial Intelligence shall never reduce the clinician's obligation to provide individualized, patient-centered care that complies with accepted standards of practice and applicable regulatory requirements.

CLINICAL DOCUMENTATION STANDARDS

Artificial Intelligence may be used to improve the quality, organization, readability, and efficiency of clinical documentation; however, the legal medical record shall always reflect the clinician's own assessment, observations, interventions, professional judgment, and services actually performed. Documentation prepared with AI assistance shall comply with all Agency documentation standards, CMS Conditions of Participation, HIPAA requirements, accreditation standards, payer requirements, and accepted professional practice standards.

All AI-assisted documentation shall be:

- Accurate.
- Complete.
- Objective.
- Patient-specific.
- Timely.

- Individualized.
- Clinically relevant.
- Consistent with physician orders.
- Consistent with the Plan of Care.
- Supported by clinician observations.
- Authenticated by the responsible workforce member.

Clinical documentation shall accurately reflect:

- Services actually performed.
- Patient condition observed during the visit.
- Interventions personally provided.
- Education actually delivered.
- Caregiver participation.
- Patient response to interventions.
- Changes in condition.
- Physician notifications.
- Coordination of care activities.
- Clinical decision-making supporting continued services.

Artificial Intelligence shall never introduce information that was not personally observed, verified, or confirmed by the responsible clinician.

Documentation shall never contain assumptions, fabricated information, generalized statements, copied patient findings, or unsupported conclusions generated by Artificial Intelligence.

Clinicians shall carefully review AI-generated documentation for indications of hallucinations, factual inaccuracies, contradictory statements, duplicated language, inappropriate terminology, or content inconsistent with the patient's clinical condition.

The responsible clinician shall revise AI-generated content whenever necessary to ensure the final documentation accurately reflects the actual services provided and meets all applicable legal, regulatory, accreditation, and Agency documentation requirements.

The Agency prohibits excessive reliance on standardized or repetitive AI-generated language that could compromise the individualized nature of the patient's medical record. Documentation shall demonstrate patient-specific assessments, individualized interventions, measurable outcomes, and clinical reasoning that supports the need for skilled home health services.

AI-assisted documentation shall be subject to routine audit through the Agency's Quality Assessment and Performance Improvement (QAPI) Program to evaluate documentation quality, accuracy, regulatory compliance, and adherence to this policy. Audit findings shall be used to identify opportunities for education, corrective action, process improvement, and ongoing competency development.

DOCUMENTATION INTEGRITY

The Home Health Agency is committed to maintaining complete, accurate, truthful, timely, and patient-specific clinical documentation that reflects the actual care provided. The integrity of the medical record is essential to patient safety, continuity of care, quality improvement, regulatory compliance, reimbursement, and the ethical practice of healthcare.

Artificial Intelligence (AI) may be used to assist in organizing, formatting, summarizing, or improving the readability of documentation; however, AI shall never replace the clinician's independent assessment, observations, professional judgment, or documentation responsibilities.

Every workforce member is responsible for ensuring that all documentation entered into the patient's legal medical record accurately reflects the care personally provided, the patient's actual condition, physician orders, and the clinician's independent professional judgment.

Documentation generated or assisted by AI shall comply with all applicable federal and state laws, CMS Conditions of Participation, HIPAA requirements, accreditation standards, payer requirements, and Agency policies.

A. Documentation Principles

All clinical documentation shall be:

- Accurate and factually correct.
- Complete and comprehensive.
- Patient-specific and individualized.
- Objective and free from unsupported opinions.
- Timely and completed in accordance with Agency policy.
- Consistent with physician orders and the Plan of Care.
- Supported by clinician observations.
- Authenticated by the responsible workforce member.
- Sufficient to support medical necessity.
- Consistent throughout the patient's medical record.

B. AI-Assisted Documentation

Artificial Intelligence may assist with:

- Organizing clinical narratives.
- Improving grammar and spelling.
- Formatting documentation.
- Summarizing clinician-entered information.
- Improving readability.
- Assisting with professional language.
- Identifying incomplete documentation for clinician review.

Artificial Intelligence shall never independently determine what occurred during a patient visit.

C. Required Human Verification

Prior to authentication, the responsible workforce member shall independently verify that AI-assisted documentation accurately reflects:

- Patient identity.
- Date and time of service.
- Assessment findings.
- Skilled services provided.
- Medications reviewed.
- Physician orders.
- Interventions performed.
- Patient response to treatment.
- Caregiver participation.
- Patient education.
- Coordination of care.
- Clinical decision-making.
- Follow-up plans.
- Visit duration, when applicable.

The responsible workforce member shall revise, edit, or remove any inaccurate, incomplete, misleading, duplicated, or unsupported AI-generated content before finalizing the medical record.

D. Prohibited Documentation Practices

The Agency strictly prohibits the use of Artificial Intelligence to:

- Create documentation for visits not performed.

- Generate assessments without personally evaluating the patient.
- Fabricate patient responses.
- Fabricate caregiver education.
- Fabricate interventions.
- Fabricate physician communications.
- Fabricate medication reconciliation.
- Fabricate vital signs.
- Fabricate wound measurements.
- Fabricate laboratory values.
- Fabricate patient progress.
- Create documentation for another clinician.
- Generate documentation for future visits.
- Modify documentation solely to support reimbursement.
- Copy documentation from another patient.
- Clone documentation between visits without appropriate updates.
- Misrepresent patient condition.
- Misrepresent services rendered.
- Conceal documentation deficiencies.
- Alter documentation after authentication without following Agency correction procedures.

E. AI Hallucinations

Artificial Intelligence may generate inaccurate, incomplete, fabricated, or misleading information, commonly referred to as "hallucinations."

Workforce members shall remain vigilant in identifying hallucinations, including:

- Incorrect medications.
- Incorrect diagnoses.
- Incorrect physician names.
- Incorrect dates.
- Unsupported clinical conclusions.
- Nonexistent interventions.
- Fabricated patient statements.
- Inaccurate coding suggestions.
- References to services not performed.

Any suspected hallucination shall be corrected immediately and, when appropriate, reported in accordance with the Agency's Incident Reporting Policy.

F. Documentation Audits

AI-assisted documentation shall be periodically reviewed through the Agency's Quality Assessment and Performance Improvement (QAPI) Program.

Audits may evaluate:

- Documentation accuracy.
- Clinical consistency.
- Individualization.
- Completeness.
- Regulatory compliance.
- Medical necessity.
- AI utilization.
- Documentation trends.
- Hallucination frequency.

- Staff compliance with this policy.

Audit findings shall be used to support education, corrective action, competency validation, and continuous quality improvement.

FRAUD, WASTE, AND ABUSE PREVENTION

The Agency maintains a zero-tolerance policy regarding fraud, waste, abuse, false claims, or other unethical activities involving the use of Artificial Intelligence.

Artificial Intelligence shall never be used to create, alter, manipulate, or enhance documentation for the purpose of obtaining reimbursement to which the Agency is not legally entitled.

All workforce members are responsible for protecting the integrity of the Medicare, Medicaid, and other third-party payer programs by ensuring documentation accurately reflects services actually provided.

A. Fraud Prevention

Artificial Intelligence shall never be used to:

- Create false documentation.
- Document services not rendered.
- Generate assessments without patient evaluation.
- Falsify visit times.
- Falsify clinician observations.
- Create physician orders.
- Modify physician orders.
- Create false patient responses.
- Fabricate coordination of care.
- Generate false supervisory visit documentation.
- Alter clinical findings after the visit to support reimbursement.

B. Waste Prevention

Artificial Intelligence shall not be used to encourage:

- Unnecessary services.
- Excessive utilization.
- Duplicate documentation.
- Redundant services.
- Inefficient care planning.
- Inappropriate scheduling.

C. Abuse Prevention

Artificial Intelligence shall never be used to:

- Upcode diagnoses.
- Downcode services.
- Increase reimbursement inappropriately.
- Justify medically unnecessary services.
- Manipulate OASIS responses.
- Alter coding recommendations without clinical support.
- Produce cloned documentation.
- Misrepresent patient acuity.
- Influence reimbursement decisions without clinical justification.

D. False Claims Prevention

Documentation prepared with AI assistance shall comply with all applicable federal and state fraud prevention laws, including the False Claims Act and applicable Medicare and Medicaid program integrity requirements.

Knowingly submitting false, misleading, or fabricated documentation may result in:

- Civil penalties.
- Criminal penalties.
- Exclusion from federal healthcare programs.
- Professional disciplinary action.
- Employment termination.
- Contract termination.
- Reporting to appropriate regulatory authorities.

E. Workforce Responsibilities

Every workforce member has an affirmative obligation to:

- Report suspected fraud, waste, or abuse.
- Report suspected AI misuse.
- Cooperate with investigations.
- Protect documentation integrity.
- Participate in required education.
- Comply with Agency compliance policies.

Individuals who report concerns in good faith shall be protected from retaliation consistent with Agency policy and applicable law.

HIPAA AND CONFIDENTIALITY

The Agency shall protect the privacy, confidentiality, integrity, and availability of Protected Health Information (PHI) when utilizing Artificial Intelligence technologies.

Artificial Intelligence shall only be used in a manner consistent with the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health (HITECH) Act, applicable state privacy laws, and Agency privacy policies.

A. Protected Health Information

Only Agency-approved Artificial Intelligence systems that satisfy applicable privacy and security requirements may be used to process Protected Health Information.

Protected Health Information shall never be entered into unauthorized public or consumer Artificial Intelligence applications.

B. Minimum Necessary Standard

When AI is used to assist workforce members, only the minimum necessary Protected Health Information required to accomplish the intended purpose shall be utilized.

C. Confidentiality

All workforce members shall maintain strict confidentiality regarding:

- Patient information.
- Employee information.
- Agency proprietary information.
- Financial information.
- Business operations.
- Vendor information.
- Quality Improvement activities.

D. Patient Rights

Patients retain all rights afforded under HIPAA, including rights related to:

- Privacy.
- Confidentiality.
- Access to records.

- Amendment requests.
- Accounting of disclosures.
- Restrictions on disclosures when applicable.

E. Access Controls

Access to AI applications containing Protected Health Information shall be limited to authorized workforce members based upon job responsibilities and the principle of least privilege.

F. Business Associate Agreements

When Artificial Intelligence vendors create, receive, maintain, or transmit Protected Health Information on behalf of the Agency, an executed Business Associate Agreement (BAA) shall be maintained in accordance with HIPAA requirements before PHI is shared.

INFORMATION SECURITY AND CYBERSECURITY

The Agency shall implement administrative, physical, and technical safeguards to protect information systems, Artificial Intelligence applications, and Protected Health Information from unauthorized access, disclosure, alteration, destruction, or cybersecurity threats.

Cybersecurity protections shall be incorporated throughout the lifecycle of all Artificial Intelligence technologies.

A. Security Requirements

Agency-approved Artificial Intelligence systems shall incorporate appropriate security measures, including:

- User authentication.
- Strong password requirements.
- Multi-factor authentication (MFA), where available.
- Encryption of data in transit and at rest.
- Role-based access controls.
- Audit logging.
- Automatic session timeouts.
- Secure data storage.
- Backup and disaster recovery capabilities.

B. Authorized Devices

Agency Artificial Intelligence systems shall be accessed only through Agency-authorized devices or approved secure remote access methods.

Use of unsecured public computers or unauthorized devices to access Agency AI systems is prohibited.

C. Mobile Device Security

Workforce members accessing AI systems through mobile devices shall comply with Agency mobile device security requirements, including:

- Password protection.
- Device encryption.
- Automatic locking.
- Remote wipe capability, when applicable.
- Software updates.
- Antivirus protection.

D. Cybersecurity Awareness

All workforce members shall receive education regarding:

- Phishing attacks.
- Social engineering.
- Malware.

- Ransomware.
- Password security.
- Safe Internet practices.
- Artificial Intelligence cybersecurity risks.
- Data protection responsibilities.

E. Incident Reporting

Any suspected cybersecurity incident involving Artificial Intelligence shall be reported immediately to the appropriate supervisor, Privacy Officer, Security Officer, or designated Agency representative in accordance with the Agency's Information Security Incident Response Policy.

AI VENDOR MANAGEMENT

The Agency shall evaluate all Artificial Intelligence vendors prior to implementation to ensure compliance with applicable legal, regulatory, operational, privacy, security, and clinical requirements. Only vendors approved through the Agency's formal evaluation process may be utilized.

A. Vendor Evaluation

The evaluation process shall include, at a minimum:

- Functional capability assessment.
- Clinical appropriateness review, when applicable.
- HIPAA compliance review.
- Privacy assessment.
- Information security assessment.
- Cybersecurity assessment.
- Data ownership review.
- Regulatory compliance review.
- Business continuity capabilities.
- Disaster recovery capabilities.
- Vendor reputation.
- Technical support capabilities.
- Service level expectations.
- Financial stability, when appropriate.

B. Data Ownership

Artificial Intelligence vendors shall acknowledge that all Agency and patient information remains the exclusive property of the Agency or the patient, as applicable.

Vendor agreements shall clearly address:

- Data ownership.
- Data retention.
- Data destruction.
- Data portability.
- Confidentiality obligations.
- Access limitations.

C. Use of Agency Data

Artificial Intelligence vendors shall not use Agency information or Protected Health Information to train, improve, or develop Artificial Intelligence models unless expressly authorized in writing by the Agency and permitted under applicable law, contractual obligations, and HIPAA requirements.

D. Ongoing Vendor Monitoring

Approved vendors shall be periodically evaluated to ensure continued compliance with:

- HIPAA.

- Agency security requirements.
- Performance expectations.
- Regulatory requirements.
- Privacy standards.
- Contractual obligations.
- Cybersecurity standards.

The Agency reserves the right to suspend, restrict, or terminate the use of any Artificial Intelligence vendor that fails to maintain acceptable levels of compliance, security, performance, patient safety, or documentation integrity.

WORKFORCE EDUCATION AND COMPETENCY

The Agency recognizes that the safe, ethical, and compliant use of Artificial Intelligence (AI) depends upon a knowledgeable and competent workforce. Accordingly, all workforce members authorized to use AI technologies shall receive education, competency validation, and ongoing training appropriate to their job responsibilities before accessing Agency-approved AI systems and at least annually thereafter.

The purpose of workforce education is to ensure that all personnel understand the capabilities, limitations, risks, responsibilities, and regulatory requirements associated with the use of Artificial Intelligence in the home health setting.

A. Initial Education

Prior to using any Agency-approved Artificial Intelligence system, workforce members shall successfully complete Agency-approved education addressing, at a minimum:

- Introduction to Artificial Intelligence.
- Agency AI policies and procedures.
- Approved and prohibited uses of AI.
- Human oversight responsibilities.
- Professional accountability.
- Clinical documentation standards.
- Documentation integrity requirements.
- Recognition of AI hallucinations and inaccuracies.
- Verification and validation of AI-generated content.
- HIPAA Privacy and Security requirements.
- Cybersecurity awareness.
- Fraud, waste, and abuse prevention.
- CMS Conditions of Participation.
- Patient confidentiality.
- Ethical use of Artificial Intelligence.
- Incident reporting procedures.

B. Annual Education

All workforce members authorized to use Artificial Intelligence shall complete annual education to reinforce Agency requirements and address:

- Regulatory updates.
- Changes to Agency policies.
- Emerging AI technologies.
- Cybersecurity threats.
- Privacy requirements.
- Lessons learned from incident investigations.

- Documentation audit findings.
- QAPI performance trends.
- Best practices for AI-assisted documentation.
- Vendor updates, when applicable.

C. Competency Validation

The Agency shall validate workforce competency through methods that may include:

- Written examinations.
- Case studies.
- Documentation review exercises.
- Practical demonstrations.
- Clinical scenarios.
- Observation of AI-assisted documentation.
- Individual performance audits.
- Supervisor evaluations.

Workforce members who do not successfully demonstrate competency shall receive additional education and remediation before continuing to utilize Artificial Intelligence technologies.

D. Ongoing Education

The Agency may provide supplemental education whenever:

- New AI systems are implemented.
- Significant regulatory changes occur.
- New cybersecurity threats are identified.
- Documentation deficiencies are identified.
- AI-related incidents occur.
- QAPI findings indicate additional education is needed.

Supervisors shall ensure staff maintain competency in accordance with this policy.

PATIENT NOTIFICATION AND TRANSPARENCY

The Agency is committed to maintaining transparency regarding the appropriate use of Artificial Intelligence while preserving patient trust, privacy, and confidence in the delivery of healthcare services.

Artificial Intelligence shall be used only as a support tool and shall never replace direct interaction between patients and qualified healthcare professionals.

Patients shall continue to receive care based upon the independent assessment, clinical judgment, and professional decision-making of licensed healthcare providers.

A. Patient Information

When appropriate and consistent with Agency policies, patients shall be informed that the Agency utilizes Artificial Intelligence technologies to assist with administrative, documentation, operational, educational, or quality improvement activities.

Patient notification may occur through:

- Admission materials.
- Patient Rights information.
- Privacy Notice.
- Agency AI disclosure forms.
- Other Agency-approved communications.

B. Patient Rights

Patients retain all rights afforded under federal and state law, including:

- Privacy.

- Confidentiality.
- Respectful treatment.
- Participation in care planning.
- Access to medical records.
- Questions regarding Agency practices.
- Filing complaints without fear of retaliation.

The use of Artificial Intelligence shall not diminish any patient right or interfere with patient-centered care.

C. Clinical Decision-Making

Patients shall be assured that:

- Licensed clinicians remain responsible for all patient care decisions.
- Artificial Intelligence does not independently diagnose, prescribe, or establish Plans of Care.
- AI-generated information is reviewed by qualified healthcare professionals before use.

The Agency shall answer patient questions regarding the appropriate use of Artificial Intelligence in accordance with Agency policies.

INCIDENT REPORTING

The Agency shall maintain a process for identifying, reporting, investigating, documenting, and resolving incidents associated with the use of Artificial Intelligence.

Prompt reporting supports patient safety, documentation integrity, regulatory compliance, quality improvement, and continuous risk reduction.

A. Reportable Incidents

Examples of reportable AI-related incidents include, but are not limited to:

- AI hallucinations affecting documentation.
- Inaccurate AI-generated clinical information.
- Unauthorized AI use.
- Privacy breaches.
- Cybersecurity incidents.
- Entry of Protected Health Information into unauthorized AI systems.
- Incorrect coding recommendations.
- Incorrect medication information.
- Documentation inconsistencies.
- Security vulnerabilities.
- AI system malfunction.
- Suspected fraud involving AI.
- Ethical concerns.
- Bias or discriminatory AI output.
- Near misses affecting patient safety.

B. Reporting Requirements

Any workforce member who identifies or suspects an AI-related incident shall immediately notify the appropriate supervisor and complete the Agency's AI Incident Report in accordance with Agency policy. Incidents involving Protected Health Information shall also be reported to the Privacy Officer.

Cybersecurity incidents shall additionally be reported to the Security Officer or designated Information Technology personnel.

C. Investigation

Reported incidents shall be investigated to determine:

- Root cause.

- Patient impact.
- Regulatory implications.
- Privacy implications.
- Documentation integrity concerns.
- Corrective actions.
- Preventive actions.
- Staff education needs.
- Vendor involvement, when applicable.

The Agency shall document all investigations and maintain records in accordance with applicable policies and regulatory requirements.

QUALITY ASSESSMENT AND PERFORMANCE IMPROVEMENT (QAPI)

Artificial Intelligence activities shall be incorporated into the Agency's Quality Assessment and Performance Improvement (QAPI) Program to ensure ongoing compliance, patient safety, documentation integrity, cybersecurity, and operational effectiveness.

The Agency shall routinely evaluate the effectiveness and safety of Artificial Intelligence technologies through performance measurement, data analysis, internal audits, and quality improvement initiatives.

A. Monitoring Activities

The QAPI Program may monitor:

- AI utilization.
- Documentation quality.
- Documentation accuracy.
- Documentation completeness.
- AI hallucination trends.
- Staff competency.
- Privacy incidents.
- Cybersecurity events.
- Coding accuracy.
- OASIS documentation trends.
- Vendor performance.
- Regulatory compliance.
- Corrective action effectiveness.
- Patient complaints related to AI use.
- Incident reporting trends.

B. Audits

The Agency may conduct periodic audits of AI-assisted documentation to evaluate:

- Compliance with Agency policy.
- Documentation integrity.
- Clinical accuracy.
- Individualization of documentation.
- Human oversight.
- Regulatory compliance.
- Medical necessity support.
- Authentication requirements.

C. Performance Improvement

When opportunities for improvement are identified, the Agency shall implement appropriate corrective actions, which may include:

- Policy revisions.
- Staff education.
- Competency validation.
- Increased documentation audits.
- Vendor reassessment.
- Process improvement initiatives.
- Enhanced cybersecurity safeguards.

QAPI findings shall be reported to the Governing Body in accordance with the Agency's Quality Assessment and Performance Improvement Plan.

ENFORCEMENT

Compliance with this policy is a condition of employment, contractual relationship, volunteer service, student participation, and authorization to utilize Agency-approved Artificial Intelligence technologies. All workforce members are expected to understand, comply with, and support the requirements established by this policy.

Failure to comply with this policy may result in corrective action appropriate to the nature and severity of the violation.

Corrective actions may include, but are not limited to:

- Verbal counseling.
- Written warning.
- Mandatory retraining.
- Competency reassessment.
- Increased documentation monitoring.
- Temporary suspension of AI access privileges.
- Removal of AI system access.
- Disciplinary action.
- Termination of employment or contractual relationship.
- Reporting to professional licensing boards, when appropriate.
- Reporting to regulatory or law enforcement agencies, when required by law.

The Agency reserves the right to immediately suspend access to Artificial Intelligence technologies whenever continued access presents a risk to patient safety, information security, documentation integrity, or regulatory compliance.

ANNUAL REVIEW

This policy shall be reviewed at least annually (as part of the Board of Director Annual meeting requirement) by the Agency Administrator, Director of Nursing, Privacy Officer, Security Officer, AI Oversight Committee, and Governing Body, or more frequently as necessary.

Review shall also occur whenever:

- Federal or state regulations change.
- CMS Conditions of Participation are revised.
- Accreditation standards are updated.
- Significant Artificial Intelligence technologies are implemented.
- Significant cybersecurity threats emerge.
- Material privacy or security incidents occur.
- AI-related patient safety events occur.
- QAPI findings indicate policy revisions are necessary.

Revisions shall be approved by the Governing Body prior to implementation.

Superseded versions of this policy shall be retained in accordance with the Agency's document control and record retention requirements.

REFERENCES

This policy is based upon applicable federal and state laws, regulations, accreditation standards, and recognized industry guidance, including but not limited to:

- Centers for Medicare & Medicaid Services (CMS), **42 CFR Part 484 – Conditions of Participation for Home Health Agencies.**
- Health Insurance Portability and Accountability Act of 1996 (HIPAA), Privacy Rule and Security Rule.
- Health Information Technology for Economic and Clinical Health (HITECH) Act.
- Federal False Claims Act (31 U.S.C. §§ 3729–3733).
- Office of Inspector General (OIG) Compliance Program Guidance.
- National Institute of Standards and Technology (NIST) Artificial Intelligence Risk Management Framework (AI RMF).
- National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF).
- Applicable state home health licensing laws and regulations.
- Agency Information Security Policy.
- Agency HIPAA Privacy and Confidentiality Policy.
- Agency Documentation Standards Policy.
- Agency Quality Assessment and Performance Improvement (QAPI) Program.
- Agency Risk Management Policy.
- Agency Incident Reporting Policy.
- Agency Fraud, Waste, and Abuse Prevention Policy.
- Agency AI Implementation Manual.
- Agency AI Staff Education and Competency Program.

APPROVAL

This policy shall become effective upon approval by the Agency Governing Body and shall remain in effect until revised or rescinded.

The Governing Body delegates responsibility for implementation, administration, monitoring, and enforcement of this policy to the Agency Administrator, with support from the Director of Nursing, Privacy Officer, Security Officer, AI Oversight Committee, and other designated leadership personnel.

The Agency shall maintain documentation of policy approval, revisions, and periodic reviews in accordance with its document control procedures.

Home Health staff Integration of Artificial Intelligence in Home Health setting (AI) Training

Part I. Artificial Intelligence Staff Education & Competency

1. Introduction to Artificial Intelligence
2. AI Fundamentals
3. AI in Home Health
4. Human Oversight
5. Professional Responsibilities
6. Documentation Integrity
7. HIPAA & Privacy
8. CMS Conditions of Participation
9. Ethical AI
10. Cybersecurity
11. Fraud, Waste & Abuse
12. Documentation Standards
13. AI Hallucinations
14. Clinical Decision Support
15. Case Studies

1. Introduction to Artificial Intelligence

Learning Objectives

Upon completion of this chapter, staff will be able to:

- Define Artificial Intelligence (AI)
- Understand how AI may be used in healthcare
- Recognize both benefits and limitations of AI
- Understand that AI never replaces licensed healthcare professionals

What is Artificial Intelligence?

Artificial Intelligence (AI) refers to computer systems designed to perform tasks that normally require human thinking. These systems can analyze information, recognize patterns, organize data, summarize information, and assist with documentation.

AI is a **tool**, not a healthcare provider.

Examples include: Drafting documentation, Summarizing information, Creating educational materials, Translating documents, Assisting with scheduling, Generating reports

AI does **not** diagnose patients or replace professional judgment.

Artificial Intelligence is a valuable tool that can improve efficiency, education, and administrative processes within a home health agency. However, AI does **not** replace licensed healthcare professionals, clinical judgment, or regulatory responsibilities. Every workforce member remains accountable for protecting patient privacy, ensuring documentation accuracy, complying with HIPAA and CMS Conditions of Participation, and maintaining the highest standards of ethical and professional practice.

2. AI Fundamentals: Artificial Intelligence (AI) refers to computer systems designed to perform tasks that normally require human intelligence, such as recognizing patterns, analyzing information, organizing data, generating written content, translating languages, and answering questions. AI learns from large amounts of data and predicts the most likely response based on patterns rather than independent reasoning.

Types of AI Commonly Used in Healthcare

- Generative AI (creates text, reports, educational materials, and summaries)
- Predictive AI (identifies trends or potential risks)
- Machine Learning (improves performance by analyzing data patterns)
- Natural Language Processing (interprets and generates human language)

AI Can Assist With: Drafting administrative documents, Creating patient education materials, Translating documents, Organizing information, Summarizing lengthy reports, Developing training materials, Supporting quality improvement activities

AI Cannot: Perform physical assessments, Replace clinical judgment, Diagnose illnesses, Prescribe treatment, Observe patient conditions, Make independent clinical decisions, Replace physician orders, AI should always be viewed as a support tool rather than a decision-maker.

3. AI in Home Health: Artificial Intelligence has many practical applications within home health agencies when used appropriately and under professional supervision.

Appropriate Uses: Developing policies and procedures, Creating orientation materials, Drafting educational handouts, Summarizing meeting minutes, Assisting with quality improvement reports, Creating competency examinations, Preparing non-clinical correspondence, Organizing agency forms

Limited Clinical Uses

AI may assist clinicians by: Organizing assessment information, Suggesting patient education topics, Identifying possible documentation omissions, Summarizing lengthy medical records

AI Should Never: Complete OASIS assessments independently, Write visit notes for visits not performed, Generate physician orders, Replace patient assessments, Determine eligibility for services, Decide patient outcomes, Replace interdisciplinary team discussions

Every clinical document must accurately reflect the clinician's own observations and professional judgment.

4. Human Oversight: Human oversight is one of the most important principles of responsible AI use.

Every AI-generated document must be reviewed by a qualified workforce member before being used.

Staff remain responsible for verifying: Accuracy, Completeness, Current regulations, Medical terminology, Medication information, Patient-specific information, Clinical appropriateness

Never assume AI information is correct simply because it appears professional.

Human oversight includes: Reading every AI-generated sentence, Correcting inaccurate information, Removing unsupported statements, Confirming information with reliable sources, Using professional judgment before implementation. The final responsibility always belongs to the clinician or employee using the AI-generated material.

5. Professional Responsibilities: Every workforce member has a professional obligation to use AI responsibly.

Employees shall: Follow agency AI policies, Protect patient confidentiality, Verify AI-generated information, Report suspected AI errors, Maintain ethical conduct, Exercise independent professional judgment

Licensed professionals remain legally responsible for: Patient assessments, Clinical decisions, Documentation, Care planning, Patient education, Communication with physicians, Regulatory compliance

Using AI never transfers accountability away from the healthcare professional.

6. Documentation Integrity: Documentation is a legal medical record and must accurately reflect services actually provided. AI may assist in improving organization or formatting but must never create fictional information.

Documentation must always be: Accurate Truthful, Complete, Objective, Timely, Patient-specific, Legible

Documentation should reflect: What was observed, What was performed, Patient response, Education provided, Physician notification when applicable

Never allow AI to: Invent assessment findings, Add symptoms not observed, Create interventions not performed, Change visit times, Generate vital signs, Create patient responses

If AI assists with drafting documentation, the clinician must review, edit, and verify every statement before signing.

7. HIPAA & Privacy: Protecting patient information is everyone's responsibility.

Protected Health Information (PHI) includes: Patient names, Dates of birth, Addresses, Telephone numbers, Medical record numbers, Insurance information, Diagnoses, Photographs, Any information that identifies a patient
Employees shall only use AI platforms approved by the agency.

Staff shall never: Copy patient records into public AI websites, Upload photographs without authorization, Share passwords, Use personal email to transmit PHI, Store confidential information in unauthorized applications

Violations of HIPAA may result in disciplinary action, civil penalties, criminal penalties, and termination.

8. CMS Conditions of Participation (CoPs): The CMS Conditions of Participation establish the minimum standards for Medicare-certified home health agencies. AI may support administrative efficiency but cannot replace regulatory requirements. Staff remain responsible for: Comprehensive patient assessments, Individualized Plans of Care, Skilled clinical judgment, Accurate documentation, Medication reconciliation, Infection prevention, Coordination of care, Patient rights, Quality Assessment and Performance Improvement (QAPI) Compliance with the CoPs requires human decision-making at every stage of patient care.

9. Ethical AI: Ethical AI means using technology in ways that protect patients, staff, and the integrity of healthcare. Core ethical principles include: Honesty, Transparency, Fairness, Privacy, Accountability, Respect for patients. Employees should disclose AI use when required by agency policy. AI should never be used to deceive patients, falsify documentation, or avoid professional responsibilities.

10. Cybersecurity: Cybersecurity protects agency information from unauthorized access. Safe AI practices include: Strong passwords, Multi-factor authentication, Agency-approved software, Updated antivirus protection, Secure Wi-Fi networks, Locked devices, Timely software updates Employees should immediately report: Suspicious emails, Unknown links, Data breaches, Lost devices, Unauthorized access attempts Cybersecurity is essential for protecting patient information and maintaining agency operations.

11. Fraud, Waste & Abuse: Improper use of AI may contribute to healthcare fraud. Examples include: Copying documentation between patients. Upcoding services, Billing for services not performed, Creating false visit notes, Altering assessments, Falsifying physician orders, Generating documentation without seeing the patient. Fraud may result in: Medicare overpayments, Civil Monetary Penalties, False Claims Act liability, Criminal prosecution, Loss of employment, Loss of professional license, Exclusion from federal healthcare programs. Every employee has a duty to report suspected fraud through agency reporting procedures.

12. Documentation Standards: Medical documentation must comply with agency policy, professional standards, state regulations, and federal requirements. Documentation should always be: Objective, Patient-specific, Accurate, Complete, Timely, Signed appropriately, Consistent with the patient's condition **Avoid:** Copy-and-paste documentation, Generic statements, Contradictory information, Unsupported conclusions. AI should only assist with drafting and organizing information after patient care has been provided.

13. AI Hallucinations: AI occasionally generates information that appears accurate but is actually incorrect. These errors are called AI hallucinations. Examples include: Incorrect medication dosages, False citations, Fabricated regulations, Incorrect physician , names, Wrong patient information, Outdated guidance, Incorrect clinical recommendations Employees should verify AI-generated information by reviewing: Agency policies, CMS regulations, Clinical references, Physician orders, Patient records. Never rely solely on AI-generated information.

14. Clinical Decision Support: AI may assist clinicians by providing educational information and identifying possible considerations. Examples include: Medication interaction alerts, Clinical guideline summaries, Patient education suggestions, Quality improvement reports AI does not determine: Diagnoses, Treatment plans, Patient eligibility, Hospitalization decisions, Discharge planning, Skilled need Clinical decisions remain the responsibility of licensed healthcare professionals using their education, experience, and patient assessment findings.

15. Case Studies:

Case Study 1: A nurse uses AI to draft patient teaching instructions regarding heart failure. Before giving the document to the patient, the nurse verifies every instruction with current physician orders.

Correct Practice: Yes

Case Study 2: A therapist copies an AI-generated treatment note directly into the medical record without reviewing the content.

Correct Practice: No. Reason: The therapist is responsible for verifying documentation before signing.

Case Study 3: An employee uploads a patient's complete medical record into an unauthorized AI website.

Correct Practice: No. Reason: This violates HIPAA and agency privacy policies.

Case Study 4: The Quality Manager uses AI to prepare a draft QAPI report. Leadership reviews, edits, and approves the final version.

Correct Practice: Yes

Part II

- Guided notes
- Exercises
- Documentation exercise
- OASIS exercises

The workbook is intended to reinforce learning, improve critical thinking, strengthen regulatory compliance, and ensure that all workforce members understand the appropriate use of AI while maintaining professional responsibility and patient safety.

Guided Notes

Purpose: Guided notes help employees actively participate during classroom instruction or self-paced learning. Instead of simply reading information, learners complete key concepts as they progress through each lesson, improving retention and understanding.

Each guided note section corresponds to the chapters presented in Volume I and includes fill-in-the-blank statements, key definitions, important regulations, and space for personal notes.

Topics Covered

- Artificial Intelligence terminology
- AI capabilities and limitations
- Human oversight responsibilities
- Documentation integrity
- HIPAA and patient privacy
- CMS Conditions of Participation
- Ethical AI practices
- Cybersecurity awareness
- Fraud, Waste & Abuse prevention
- AI hallucinations
- Clinical decision support

Learning Objective

At the completion of this section, employees should be able to summarize each major concept in their own words and identify how AI may be appropriately used within the agency.

Practical Exercises

Purpose: Practical exercises provide employees with opportunities to apply AI concepts to realistic workplace situations. These activities encourage critical thinking and reinforce agency policies regarding the safe and appropriate use of Artificial Intelligence.

Exercises may include:

- Identifying appropriate and inappropriate AI use
- Selecting the correct response to workplace scenarios
- Determining when human review is required

- Evaluating AI-generated responses
- Applying agency AI policies

Examples

- Can AI prepare patient education materials?
- Should AI complete an OASIS assessment?
- Is it acceptable to copy AI-generated documentation directly into the medical record?
- Should AI replace nursing judgment?

Exercise: Identifying Appropriate and Inappropriate AI Use

Purpose: This exercise helps employees recognize when the use of Artificial Intelligence (AI) is appropriate and when it is prohibited in the home health setting. Understanding these distinctions is essential to protect patient safety, maintain documentation integrity, safeguard confidential information, and ensure compliance with HIPAA, CMS Conditions of Participation (CoPs), state regulations, and agency policies.

AI is intended to **support** healthcare professionals—not replace their education, experience, clinical judgment, or professional responsibilities.

Learning Objectives: Upon completion of this exercise, participants will be able to:

- Differentiate between appropriate and inappropriate uses of AI.
- Apply agency policies regarding AI use.
- Recognize situations that require human clinical judgment.
- Protect patient confidentiality when using AI.
- Identify activities that may result in regulatory noncompliance or fraud if AI is used improperly.

Appropriate Uses of AI: The following are examples of acceptable uses of AI when performed in accordance with agency policy and under appropriate human oversight:

- Assisting with the development of agency policies and procedures.
- Creating employee orientation and educational materials.
- Preparing patient education handouts that are reviewed for accuracy before distribution.
- Drafting non-clinical letters, emails, or administrative documents.
- Summarizing lengthy regulations or guidance documents for educational purposes.
- Assisting with Quality Assessment and Performance Improvement (QAPI) reports.
- Developing staff competency tests, quizzes, and training materials.
- Organizing meeting notes or committee minutes.
- Creating templates or checklists for administrative use.
- Translating non-clinical documents after review for accuracy.
- Assisting clinicians in organizing documentation before final review and completion.

Remember: All AI-generated content must be reviewed, edited, verified, and approved by a qualified employee before it is used or distributed.

Inappropriate Uses of AI: The following activities are prohibited because they compromise patient safety, documentation integrity, or regulatory compliance:

- Completing a patient assessment without personally evaluating the patient.
- Writing a visit note for services that were not performed.
- Creating assessment findings that were not observed by the clinician.
- Fabricating vital signs, wounds, symptoms, or patient responses.
- Completing or modifying OASIS assessments without an independent clinical assessment.
- Creating or changing physician orders.
- Making clinical decisions without professional review.
- Determining patient eligibility for services.
- Copying AI-generated documentation directly into the medical record without verification.
- Uploading Protected Health Information (PHI) into unauthorized AI platforms.
- Using AI to justify billing for services not provided.
- Altering documentation to increase reimbursement or support a higher level of care.

- Replacing professional nursing, therapy, social work, or physician judgment with AI recommendations. These practices may violate agency policy, HIPAA, Medicare regulations, professional standards, and federal fraud and abuse laws.

Human Oversight Reminder: Every workforce member is responsible for ensuring that AI-generated information is: Accurate, Patient-specific, Complete, Clinically appropriate, Supported by actual patient observations, Consistent with physician orders and the Plan of Care, Compliant with agency policy and regulatory requirements. **The healthcare professional** -not the AI system- remains legally and professionally accountable for all documentation, clinical decisions, and patient care.

Human oversight is required whenever Artificial Intelligence (AI) is used because AI is a support tool—not a licensed healthcare professional. Although AI can analyze information, organize data, and generate text, it cannot independently verify facts, assess patients, apply clinical judgment, or accept legal and professional responsibility for patient care. Qualified workforce members must review and validate all AI-generated information before it is used.

Practice Activity

Read each scenario below and determine whether the use of AI is **Appropriate** or **Inappropriate**. Be prepared to explain your answer.

Scenario	Appropriate	Inappropriate
AI is used to draft an employee in-service presentation that is reviewed by the educator before use.	☐	☐
A nurse copies AI-generated documentation into the medical record without reading it.	☐	☐
AI helps summarize a CMS regulation for staff education.	☐	☐
A therapist uses AI to create documentation for a home visit that never occurred.	☐	☐
An administrator uses AI to draft a Quality Improvement report that is reviewed and approved before submission.	☐	☐
An employee enters a patient's full medical record into a public AI website.	☐	☐
AI is used to prepare a patient education brochure that is reviewed by a clinician before distribution.	☐	☐
AI recommends a diagnosis, and the clinician accepts it without performing an assessment.	☐	☐

Discussion Questions

1. Why is human oversight required whenever AI is used?
2. What risks exist if AI-generated information is accepted without verification?
3. How can inappropriate AI use affect patient safety and quality of care?
4. Which regulations or agency policies could be violated by improper AI use?
5. What should you do if you discover that AI-generated documentation contains inaccurate or fabricated information?

Human oversight is required whenever Artificial Intelligence (AI) is used because AI is a support tool—not a licensed healthcare professional. Although AI can analyze information, organize data, and generate text, it cannot independently verify facts, assess patients, apply clinical judgment, or accept legal and professional responsibility for patient care. Qualified workforce members must review and validate all AI-generated information before it is used.

Human oversight is essential to:

- Ensure the accuracy, completeness, and reliability of AI-generated information.
- Detect and correct AI errors, hallucinations, outdated information, or fabricated content.

- Confirm that documentation accurately reflects the patient's condition, services provided, and the clinician's own observations.
- Protect patient safety by preventing inappropriate clinical decisions based on inaccurate information.
- Ensure compliance with HIPAA, CMS Conditions of Participation (CoPs), state regulations, accreditation standards, and agency policies.
- Verify that documentation is patient-specific and does not contain copied, generic, or unsupported statements.
- Protect the confidentiality and security of Protected Health Information (PHI).
- Prevent fraud, waste, and abuse by ensuring documentation supports only services that were actually provided.
- Maintain the integrity of the medical record and support continuity of care among members of the interdisciplinary team.
- Ensure that ethical standards and professional responsibilities are maintained at all times.

AI can assist with administrative tasks, education, organization, and documentation support, but it **cannot replace the knowledge, experience, critical thinking, or professional judgment of licensed healthcare professionals**. The clinician or employee using AI remains fully responsible for reviewing, correcting, approving, and taking accountability for all AI-assisted work before it is used in patient care, documentation, billing, or agency operations.

Accepting AI-generated information without verification can create significant risks for patients, healthcare professionals, and the home health agency. AI systems may generate inaccurate, incomplete, outdated, or fabricated information (known as **AI hallucinations**) that appears credible but is not supported by clinical evidence or regulatory requirements.

Potential risks include:

- Compromised patient safety due to incorrect clinical information or recommendations.
- Inaccurate or incomplete medical documentation that does not reflect the patient's actual condition or the care provided.
- Clinical decisions based on false or misleading information.
- Medication errors resulting from incorrect drug names, dosages, or interactions.
- HIPAA violations if Protected Health Information (PHI) is entered into unauthorized AI platforms.
- Noncompliance with CMS Conditions of Participation (CoPs), state regulations, accreditation standards, and agency policies.
- Billing errors, overpayments, or allegations of fraud if inaccurate documentation supports claims for services not provided or services that are not medically necessary.
- Survey deficiencies, corrective action plans, civil monetary penalties, repayment of Medicare or Medicaid funds, loss of accreditation, or legal liability.
- Damage to the agency's reputation and loss of patient trust.
- Professional disciplinary action, including corrective counseling, suspension, termination of employment, or licensure action against the responsible healthcare professional.

Because AI cannot independently verify facts or exercise professional clinical judgment, **every AI-generated document, recommendation, or response must be carefully reviewed, validated, and approved by a qualified workforce member before it is used for patient care, documentation, education, billing, or operational decisions**. The licensed healthcare professional remains fully responsible for the accuracy and appropriateness of all information used in the delivery of patient care.

Inappropriate use of Artificial Intelligence (AI) can negatively affect patient safety and the quality of care by introducing inaccurate, incomplete, or misleading information into the clinical decision-making process. AI is not capable of performing patient assessments, observing changes in a patient's condition, or applying professional clinical judgment. When AI is used beyond its intended purpose or without proper human oversight, it may contribute to unsafe patient care and regulatory noncompliance.

Potential impacts on patient safety and quality of care include:

- Delayed recognition of changes in a patient's condition that require immediate intervention.
- Incorrect or incomplete assessments that result in inappropriate care planning.
- Medication errors caused by inaccurate medication lists, dosages, or drug interaction information.

- Failure to identify patient-specific risks such as falls, infections, wounds, or changes in functional status.
- Inaccurate or fabricated documentation that does not reflect the actual care provided.
- Poor communication among members of the interdisciplinary team due to incorrect documentation.
- Failure to notify the physician of significant changes in the patient's condition.
- Inappropriate clinical decisions based on incorrect AI-generated recommendations.
- Loss of continuity of care when documentation is incomplete or inconsistent.
- Reduced patient confidence and trust in the healthcare team.
- Deficiencies during CMS, state, or accreditation surveys due to documentation errors or failure to meet regulatory requirements.

To protect patient safety, AI should only be used as a supportive tool. All AI-generated information must be carefully reviewed, verified, and, when necessary, corrected by a qualified healthcare professional before it is incorporated into patient care or the medical record. Clinical assessments, treatment decisions, documentation, and patient education must always be based on the clinician's own observations, professional judgment, and applicable standards of practice.

Improper use of Artificial Intelligence (AI) may violate numerous federal and state regulations, accreditation standards, professional practice requirements, and agency policies. Because AI cannot assume legal or professional responsibility, workforce members remain accountable for ensuring that all AI-assisted activities comply with applicable laws and organizational requirements.

Examples of regulations and policies that may be violated include:

Federal Regulations

- **HIPAA Privacy Rule** – If Protected Health Information (PHI) is disclosed or entered into unauthorized AI platforms without appropriate safeguards or authorization.
- **HIPAA Security Rule** – If electronic PHI is not adequately protected from unauthorized access, disclosure, or cybersecurity threats.
- **CMS Conditions of Participation (42 CFR Part 484)** – If AI is used in a manner that compromises patient assessments, individualized plans of care, documentation accuracy, coordination of care, patient rights, or quality of care.
- **False Claims Act (31 U.S.C. §§ 3729–3733)** – If AI-generated documentation is used to support billing for services that were not provided or are inaccurately documented.
- **Federal Fraud, Waste, and Abuse Laws** – If AI contributes to false documentation, upcoding, duplicate documentation, unnecessary services, or other fraudulent billing practices.

State and Professional Requirements

Improper AI use may also violate: State home health agency regulations., State licensing board standards of professional practice, Professional codes of ethics for nurses, therapists, social workers, and other licensed healthcare professionals. Medical record documentation requirements established by federal and state law.

Agency Policies

Employees may also violate agency policies related to:

- Artificial Intelligence (AI) Use Policy.
- Documentation and Clinical Record Integrity.
- HIPAA Privacy and Confidentiality.
- Information Security and Cybersecurity.
- Acceptable Use of Technology.
- Documentation Standards.
- Quality Assessment and Performance Improvement (QAPI).
- Fraud, Waste, and Abuse Prevention.
- Employee Code of Conduct and Professional Ethics.
- Patient Rights and Confidentiality.

Potential Consequences

Failure to comply with these regulations and policies may result in:

- Patient harm or compromised quality of care.
- HIPAA investigations and civil penalties.
- CMS survey deficiencies and corrective action plans.

- Medicare or Medicaid payment denials or recoupments.
- Civil or criminal liability for fraud.
- Disciplinary action by the agency.
- Professional licensure investigations or sanctions.
- Loss of accreditation or participation in federal healthcare programs.

All workforce members are responsible for using AI only in accordance with applicable laws, regulatory requirements, accreditation standards, and agency policies. AI should enhance—not replace—professional judgment, ethical decision-making, and compliance with healthcare regulations.

If you discover that AI-generated documentation contains inaccurate, incomplete, misleading, or fabricated information, you should **never use or sign the documentation in its current form**. AI-generated content must always be carefully reviewed and verified before it becomes part of the patient's medical record or is used for clinical, administrative, or billing purposes.

The appropriate steps include:

1. **Stop using the document immediately.** Do not copy, submit, sign, or place inaccurate AI-generated information into the patient's medical record.
2. **Verify the information.** Compare the AI-generated content with the patient's medical record, physician orders, assessment findings, medication list, Plan of Care, and other reliable clinical sources.
3. **Correct all inaccuracies.** Remove any fabricated, unsupported, outdated, or incorrect information and replace it with accurate, patient-specific information based on your own assessment and verified clinical documentation.
4. **Ensure the documentation reflects actual care provided.** The medical record must accurately describe the services performed, the patient's condition, interventions provided, patient response, and any required physician notifications.
5. **Notify your supervisor if necessary.** If the error could affect patient safety, documentation integrity, billing, regulatory compliance, or indicates misuse of AI, promptly report the concern to your supervisor, Clinical Manager, Privacy Officer, Compliance Officer, or other designated agency representative in accordance with agency policy.
6. **Do not rely on AI to correct its own errors without verification.** Any revised AI-generated content must also be reviewed and validated by a qualified healthcare professional.
7. **Report repeated or significant AI issues.** If you identify recurring inaccuracies, fabricated information, or unsafe AI behavior, report the issue through the agency's quality improvement, compliance, or incident reporting process so corrective action can be taken.

Key Principle

The licensed healthcare professional is ultimately responsible for the accuracy, completeness, and integrity of all documentation. AI may assist with drafting or organizing information, but it **cannot verify clinical facts, replace professional judgment, or assume legal responsibility for the medical record**. Only verified, accurate, and patient-specific information should be included in the patient's documentation.

Key Takeaway

Artificial Intelligence is a valuable support tool that can improve efficiency and productivity; however, it must never replace professional judgment, patient assessment, ethical decision-making, or regulatory compliance.

Employees are responsible for ensuring that every use of AI is appropriate, accurate, secure, and consistent with agency policy and the standards of professional practice.

Documentation Exercise

Purpose

This exercise is designed to help employees recognize common documentation errors that may occur when Artificial Intelligence (AI) is used improperly in the home health setting. Participants will evaluate AI-generated documentation, identify deficiencies, and revise the documentation to ensure it complies with agency policy, CMS Conditions of Participation (CoPs), HIPAA requirements, professional standards, and documentation best practices.

Learning Objectives

Upon completion of this exercise, participants will be able to:

- Identify inaccurate, incomplete, or fabricated AI-generated documentation.
- Differentiate between objective observations and unsupported statements.
- Recognize documentation that lacks patient-specific information.
- Apply proper documentation standards to clinical records.
- Understand the importance of clinician review before using AI-assisted documentation.

Instructions

Read each sample documentation note carefully.

For each scenario:

1. Identify all documentation deficiencies.
2. Explain why the documentation is incorrect.
3. Rewrite the note using accurate, objective, patient-specific documentation.
4. Discuss whether the documentation should be accepted into the medical record.

Scenario 1 – Skilled Nursing Visit

AI-Generated Documentation

"Patient is doing well today. Vital signs are normal. Wound looks better. Patient understands education provided. Continue current treatment."

Identify the Documentation Problems

- ☐ Vital signs are not documented.
- ☐ Wound assessment lacks measurable findings.
- ☐ No patient-specific information.
- ☐ Education is not described.
- ☐ Patient response is not documented.
- ☐ No skilled nursing interventions documented.
- ☐ Documentation is vague and subjective.
- ☐ Other: _____

Questions

1. Why is this documentation insufficient?

This documentation is insufficient because it is **vague, incomplete, and not patient-specific**. It does not provide enough objective clinical information to accurately describe the patient's condition, the skilled nursing services provided, or the patient's response to treatment. Medical documentation must clearly demonstrate the need for skilled nursing services, support continuity of care, and meet regulatory and reimbursement requirements.

The documentation is deficient because it:

- Fails to record the patient's actual vital signs (blood pressure, pulse, respirations, temperature, oxygen saturation, etc.).
- Does not include a detailed wound assessment, such as wound location, measurements, drainage, tissue appearance, odor, or signs of infection.
- Uses subjective phrases such as "doing well" and "looks better" without objective clinical evidence.
- Does not describe the skilled nursing interventions performed during the visit.
- Fails to specify the education provided to the patient or caregiver.
- Does not document the patient's understanding or response to the education.
- Does not indicate whether medications were reviewed or if changes in the patient's condition were identified.
- Does not identify communication with the physician when required.
- Does not support the medical necessity for continued skilled nursing services.

Because the documentation lacks objective findings and patient-specific details, it does not accurately reflect the care provided and may fail to meet agency policy, professional documentation standards, CMS Conditions of

Participation (42 CFR Part 484), Medicare documentation requirements, and accepted standards of clinical practice. All documentation must be accurate, complete, objective, timely, and based on the clinician's own assessment and observations.

2. What information is missing?

The documentation is missing several essential elements required to create a complete, accurate, and patient-specific skilled nursing note. A home health visit note should clearly describe the patient's condition, the skilled services provided, and the patient's response to care.

The following information is missing:

- **Objective assessment findings**, including the patient's general condition and any significant changes since the previous visit.
- **Complete vital signs**, such as blood pressure, pulse, respiratory rate, temperature, oxygen saturation, pain level, and blood glucose (if applicable).
- **Detailed wound assessment**, including the wound location, measurements (length, width, depth), drainage, tissue appearance, odor, surrounding skin condition, and signs or symptoms of infection.
- **Skilled nursing interventions** performed during the visit, such as wound care, medication management, assessment, patient monitoring, or other skilled procedures.
- **Medication review**, including reconciliation, patient compliance, adverse reactions, medication changes, and any education provided.
- **Patient and/or caregiver education**, including the specific topics taught (e.g., medication management, wound care, infection prevention, fall prevention), and the patient's or caregiver's understanding using methods such as teach-back.
- **Patient response to treatment and education**, including tolerance of procedures, progress toward goals, and any questions or concerns expressed by the patient or caregiver.
- **Communication with the physician or interdisciplinary team**, if there were significant findings, changes in condition, abnormal results, or requests for new orders.
- **Plan for the next visit**, including ongoing skilled needs, follow-up interventions, and any additional monitoring required.
- **Evidence supporting the continued need for skilled nursing services**, demonstrating why the patient's condition requires the knowledge and skills of a licensed nurse.

Complete documentation should be **objective, accurate, timely, patient-specific, and clearly demonstrate the skilled services provided and the patient's response to care**, while supporting continuity of care and compliance with agency policy and CMS Conditions of Participation.

3. Rewrite the note using objective clinical documentation.

4. **Sample Revised Skilled Nursing Documentation**

5. **Skilled Nursing Visit Note**

6. Skilled nursing visit completed as ordered. Patient was alert and oriented to person, place, time, and situation, resting comfortably at home and in no acute distress. Vital signs obtained: Blood Pressure **128/76 mmHg**, Pulse **78 bpm**, Respiratory Rate **18 breaths/min**, Temperature **98.4°F**, Oxygen Saturation **97% on room air**, and Pain **2/10**. Vital signs were within the patient's established parameters.
7. Wound assessment performed to the **left lower leg**. Wound measured **2.5 cm (L) × 1.8 cm (W) × 0.2 cm (D)**. Wound bed consisted of approximately **90% healthy granulation tissue** and **10% yellow slough**. Small amount of serous drainage noted without foul odor. Surrounding skin intact with no erythema, warmth, edema, or other signs of infection. Wound cleansed with normal saline and dressing changed according to physician orders using sterile technique. Patient tolerated the procedure without complications.
8. Medication reconciliation completed. Patient reported taking all prescribed medications as directed and denied missed doses or adverse medication effects. No discrepancies identified between the medication list and the physician's orders.
9. Patient and caregiver were instructed on proper wound care, recognizing signs and symptoms of infection, medication adherence, adequate nutrition to support wound healing, and the importance of reporting increased pain, redness, swelling, drainage, fever, or other changes in condition. Patient and caregiver demonstrated understanding through the teach-back method and were able to verbalize when to contact the agency or physician.

10. Patient remains homebound and continues to require skilled nursing services for ongoing wound assessment, wound care, medication monitoring, patient education, and evaluation of treatment effectiveness. No immediate physician notification was required at this visit. Plan is to continue skilled nursing visits as ordered to monitor wound healing, reinforce education, and assess for any changes in the patient's condition.

Scenario 2 – Home Health Aide Visit

AI-Generated Documentation

"Patient received personal care. Everything went well."

Identify the Documentation Problems

- ☐ Does not describe services provided.
- ☐ No patient response documented.
- ☐ No changes in patient condition.
- ☐ No safety observations.
- ☐ No patient participation documented.
- ☐ Documentation is too general.

This documentation is incomplete and does not meet home health documentation standards because it fails to describe the care that was actually provided or the patient's condition during the visit.

Mark all applicable deficiencies:

- ☒ Does not identify the specific personal care services provided (e.g., bathing, dressing, grooming, toileting, oral hygiene, shampooing, skin care).
- ☒ Does not document the patient's functional status or the level of assistance required (independent, supervision, standby assist, one-person assist, total assist).
- ☒ Does not describe the patient's response to the services provided.
- ☒ Does not document changes in the patient's physical or mental condition.
- ☒ Does not include skin observations or report any redness, bruising, open areas, or other abnormalities, when applicable.
- ☒ Does not document mobility or transfer assistance provided.
- ☒ Does not indicate whether safety precautions or fall prevention measures were followed.
- ☒ Does not identify whether the patient's home environment was observed to be safe.
- ☒ Does not document patient participation, tolerance of care, or any complaints of pain or discomfort.
- ☒ Does not report any concerns that should be communicated to the supervising nurse or therapist.
- ☒ Uses vague, non-specific language ("Everything went well") that does not objectively describe the visit.
- ☒ Documentation is not patient-specific and does not demonstrate that the services outlined in the Home Health Aide Care Plan were completed.

Key Learning Point

Home Health Aide documentation must clearly describe the **services provided**, the **patient's condition before, during, and after care**, the **level of assistance required**, the **patient's response to care**, and **any observations or changes that should be reported to the supervising clinician**. Documentation should always be objective, complete, accurate, and patient-specific.

Questions

What additional information should be documented?

A Home Health Aide visit note should provide a clear, accurate, and patient-specific description of the care provided and the patient's condition during the visit. The documentation should demonstrate that the services outlined in the Home Health Aide Care Plan were performed and should include any observations that need to be reported to the supervising nurse or therapist.

The following additional information should be documented:

- **Date and time of the visit**, including the duration of services provided.

- **Patient's condition upon arrival**, including alertness, orientation, general appearance, and any complaints of pain or discomfort.
- **Specific personal care services provided**, such as bathing, dressing, grooming, oral hygiene, shampooing, shaving, toileting, incontinent care, skin care, nail care (if permitted), and assistance with eating or hydration.
- **Level of assistance required**, such as independent, supervision, standby assistance, one-person assist, two-person assist, or total assistance.
- **Mobility and transfer assistance** provided, including the use of assistive devices such as a walker, wheelchair, gait belt, or cane.
- **Patient tolerance and response** to the care provided, including any signs of fatigue, pain, shortness of breath, dizziness, or refusal of care.
- **Observations of the patient's skin condition**, including redness, bruising, swelling, open areas, pressure injuries, rashes, or other abnormalities that should be reported.
- **Safety observations**, including environmental hazards, fall risks, and whether the patient's home environment remained safe during the visit.
- **Changes in the patient's physical, cognitive, or emotional condition** observed during the visit.
- **Patient and caregiver participation**, cooperation, and any education or reminders provided within the aide's scope of practice, such as reinforcing instructions previously provided by the supervising clinician.
- **Communication with the supervising nurse or therapist**, including documentation of any significant findings or concerns that required reporting according to agency policy.
- **Patient's condition at the end of the visit**, confirming that the patient was safe, comfortable, and left in an appropriate environment.

Complete Home Health Aide documentation should be **objective, accurate, timely, patient-specific, and consistent with the Home Health Aide Care Plan**, while providing sufficient information to support continuity of care and effective communication among the interdisciplinary team.

Scenario 3 – Physical Therapy Visit

AI-Generated Documentation

"Patient walked better today."

Identify the Documentation Problems

- ☐ No distance documented.
- ☐ No assistance level documented.
- ☐ No assistive device identified.
- ☐ No balance assessment.
- ☐ No patient tolerance documented.
- ☐ No skilled interventions documented.

Rewrite the Documentation

Sample Revised Physical Therapy Documentation

Physical Therapy Visit Note

Physical therapy visit completed as ordered. Patient was alert and oriented to person, place, time, and situation and denied new pain or recent falls since the previous visit. Patient reported mild fatigue but was motivated to participate in the therapy session.

Therapeutic exercises were performed to improve lower extremity strength, balance, endurance, and functional mobility. Patient completed seated and standing strengthening exercises, including hip flexion, knee extension, ankle pumps, mini-squats, and sit-to-stand exercises with verbal cueing for proper body mechanics.

Gait training was performed using a **front-wheeled walker** on a level surface. Patient ambulated **150 feet** with **standby assistance**, demonstrating improved gait stability compared to the previous visit. Mild decrease in step length and gait speed was noted, but no loss of balance occurred during ambulation. Verbal cues were provided to encourage an upright posture, proper walker placement, and safe turning techniques.

Transfer training was completed for sit-to-stand and stand-to-sit activities. Patient required **supervision with occasional verbal cueing** to ensure safe hand placement and controlled movements. Patient tolerated the treatment session well with only mild fatigue, which resolved after a brief rest period. No complaints of dizziness, chest pain, or shortness of breath were reported during therapy. Patient was educated on the home exercise program, fall prevention strategies, energy conservation techniques, and the importance of using the walker during all ambulation. The patient demonstrated understanding by correctly performing the prescribed exercises and verbalizing appropriate safety precautions. The patient continues to demonstrate progress toward established therapy goals but remains at risk for falls due to decreased lower extremity strength and balance deficits. Continued skilled physical therapy is medically necessary to improve strength, gait, balance, functional mobility, and independence with activities of daily living while reducing the risk of falls. The plan is to continue therapy as ordered and progress exercises and gait training as tolerated.

Scenario 4 – Medication Review

AI-Generated Documentation

"Medications reviewed. No problems noted."

Identify the Documentation Problems

- ☐ No medication reconciliation documented.
- ☐ No verification with physician orders.
- ☐ No adverse effects assessed.
- ☐ No medication education documented.
- ☐ No patient understanding documented.
- ☐ No follow-up required.

Discussion

Why is medication documentation important?

Medication documentation is an essential component of safe, high-quality home health care. Accurate and complete medication documentation helps ensure that patients receive the correct medications as prescribed, supports continuity of care among healthcare providers, and reduces the risk of medication-related complications. It also demonstrates compliance with agency policy, professional standards, and CMS Conditions of Participation (CoPs).

Proper medication documentation is important because it:

- Verifies that a comprehensive medication review and reconciliation were completed using the physician's orders and the medications available in the patient's home.
- Identifies medication discrepancies, such as omitted medications, duplicate therapies, incorrect dosages, expired medications, or medications being taken differently than prescribed.
- Assesses the patient's understanding of each medication, including its purpose, dosage, frequency, route, and potential side effects.
- Evaluates medication adherence and identifies barriers that may affect the patient's ability to take medications correctly.
- Identifies potential adverse drug reactions, allergies, contraindications, and clinically significant drug-to-drug or drug-to-food interactions.
- Documents medication education provided to the patient and/or caregiver and their understanding of the instructions using methods such as teach-back.
- Identifies the need for physician notification when medication discrepancies, adverse reactions, or other concerns are discovered.
- Supports patient safety by helping prevent medication errors, hospitalizations, emergency department visits, and avoidable adverse events.
- Provides clear communication among members of the interdisciplinary team, ensuring that all clinicians have current and accurate medication information.

- Supports regulatory compliance, quality improvement activities, and reimbursement by demonstrating that medication management services were performed appropriately.

A statement such as **"Medications reviewed. No problems noted."** is not sufficient because it does not describe **what medications were reviewed, how the review was conducted, whether reconciliation was completed, if the patient was taking the medications correctly, whether education was provided, or whether any follow-up actions were required.** Complete medication documentation should be specific, objective, patient-centered, and accurately reflect the clinician's assessment and interventions during the visit.

Documentation Review Checklist

When reviewing AI-assisted documentation, ask yourself:

Review Item	Yes	No
Is the documentation patient-specific?	☐	☐
Does it accurately reflect the care provided?	☐	☐
Are assessment findings objective?	☐	☐
Are all interventions documented?	☐	☐
Is the patient's response included?	☐	☐
Are medications documented accurately?	☐	☐
Is physician notification documented, when applicable?	☐	☐
Is the note free of unsupported statements?	☐	☐
Has the documentation been reviewed by the clinician?	☐	☐

Group Discussion

Discuss the following questions:

1. Which documentation deficiencies were most difficult to identify?

The documentation deficiencies that are often the most difficult to identify are those that appear complete at first glance but lack the objective, patient-specific details necessary to accurately describe the patient's condition and the skilled services provided. General statements or well-written AI-generated text may sound professional, yet fail to meet clinical documentation standards.

Examples of commonly overlooked deficiencies include:

- Vague or subjective statements such as *"patient is doing well," "wound looks better,"* or *"tolerated treatment well"* without objective clinical evidence.
- Missing patient-specific assessment findings, including measurable observations, vital signs, wound measurements, or functional status.
- Failure to document the patient's response to treatment or education provided during the visit.
- Lack of evidence supporting the continued need for skilled services and home health eligibility.
- Missing medication reconciliation details, including discrepancies, adverse effects, patient adherence, or education provided.
- Failure to document communication with the physician regarding significant findings or changes in the patient's condition.
- Generic documentation that could apply to any patient rather than reflecting the individual's unique condition and care needs.
- Inconsistencies between the documentation, physician's orders, Plan of Care, and the services actually performed.
- Missing documentation of clinical reasoning and the skilled interventions that justify the involvement of a licensed healthcare professional.

These deficiencies are particularly challenging because AI-generated documentation may be grammatically correct and professionally written while still omitting critical clinical information. Healthcare professionals must carefully review every note to ensure it is **accurate, objective, complete, patient-specific, and supported by their own assessment and observations**, rather than relying solely on how well the documentation reads.

2. How could these errors affect patient safety?

Documentation errors can have a significant impact on patient safety because the medical record serves as the primary source of communication among members of the interdisciplinary team. Inaccurate, incomplete, or misleading documentation may result in inappropriate clinical decisions, delays in treatment, medication errors, and a failure to recognize changes in the patient's condition.

These errors can affect patient safety by:

- Delaying the identification and treatment of changes in the patient's condition.
- Contributing to medication errors due to incomplete or inaccurate medication documentation.
- Resulting in inappropriate or ineffective treatment plans because the patient's condition is not accurately documented.
- Preventing other clinicians from understanding the patient's current status, progress, or care needs.
- Causing important symptoms, complications, or safety concerns to go unrecognized or unreported.
- Increasing the risk of falls, infections, pressure injuries, hospitalizations, or other preventable adverse events.
- Failing to document or communicate the need for physician notification when significant findings are identified.
- Interrupting continuity of care by providing incomplete or inconsistent information to the interdisciplinary team.
- Leading to duplicate services or missed interventions because previous care was not accurately recorded.
- Reducing the ability of the healthcare team to evaluate the effectiveness of treatments and make appropriate adjustments to the Plan of Care.

When documentation errors result from improper use of Artificial Intelligence, the risks may be even greater if fabricated, outdated, or inaccurate information is accepted without verification. For this reason, **all AI-generated documentation must be carefully reviewed, validated, and corrected by the healthcare professional before it is entered into the patient's medical record.** Accurate, objective, and patient-specific documentation is essential to ensure safe, effective, and high-quality patient care.

3. How could these deficiencies affect reimbursement or survey compliance?

Documentation deficiencies can significantly affect both **Medicare reimbursement** and **survey compliance** because the medical record is the primary evidence that services were medically necessary, properly provided, and documented in accordance with federal regulations. Incomplete, inaccurate, or unsupported documentation may result in payment denials, survey deficiencies, corrective actions, and legal or financial consequences for the agency.

Documentation deficiencies may result in:

- **Denial of Medicare or other third-party payer claims** due to insufficient documentation supporting the services billed.
- **Recoupment of payments** if an audit determines that documentation does not support medical necessity or the skilled services provided.
- **Survey deficiencies** during CMS, state, or accreditation surveys for failure to comply with documentation requirements and the CMS Conditions of Participation (CoPs).
- **Plans of Correction (POCs)** and increased regulatory oversight following identified deficiencies.
- **Reduced quality outcomes** and negative performance indicators that may affect the agency's Quality Assessment and Performance Improvement (QAPI) program.
- **Failure to demonstrate medical necessity**, homebound status, skilled need, or patient progress toward established goals.
- **Increased risk of allegations of fraud, waste, or abuse** if documentation is inaccurate, duplicated, fabricated, or does not accurately reflect the care provided.
- **Civil monetary penalties, repayment obligations, or exclusion from federal healthcare programs** when documentation deficiencies are associated with false claims or other regulatory violations.
- **Damage to the agency's accreditation status and reputation**, potentially affecting patient confidence and referral relationships.

Accurate, complete, objective, and patient-specific documentation is essential to demonstrate that services were medically necessary, delivered as ordered, and met applicable professional and regulatory standards. Every clinician is responsible for ensuring that documentation supports the care provided and complies with agency policy, CMS Conditions of Participation, payer requirements, and accepted standards of clinical practice.

4. What role should AI play in clinical documentation?

Artificial Intelligence (AI) should serve as a **supportive documentation tool** that assists healthcare professionals in improving efficiency, organization, and consistency while maintaining the accuracy and integrity of the medical record. AI may help draft documentation, organize information, summarize clinical data, identify potential omissions, and improve the clarity of written documentation. However, AI **must never replace the clinician's independent assessment, critical thinking, clinical judgment, or professional responsibility**.

The appropriate role of AI in clinical documentation includes:

- Assisting with organizing and formatting documentation.
- Helping draft clinical narratives after the clinician has completed the patient assessment.
- Identifying potential documentation omissions or inconsistencies for clinician review.
- Assisting with grammar, spelling, and readability.
- Summarizing lengthy clinical information to improve efficiency.
- Supporting documentation quality improvement initiatives.
- Assisting with the preparation of patient education materials and non-clinical documentation.

AI **must not** be used to:

- Perform or replace patient assessments.
- Create documentation for services that were not provided.
- Fabricate assessment findings, vital signs, patient responses, or interventions.
- Complete OASIS assessments independently.
- Generate or alter physician orders.
- Make clinical decisions or determine the patient's plan of care.
- Copy generic documentation into multiple patient records without individualization.
- Replace the clinician's professional judgment or legal responsibility.

Before any AI-assisted documentation becomes part of the medical record, the healthcare professional must:

- Review every statement for accuracy and completeness.
- Verify that all information is supported by the patient's assessment and physician orders.
- Correct any inaccurate, outdated, or fabricated information.
- Ensure the documentation is objective, patient-specific, and reflects the actual care provided.
- Confirm compliance with agency policy, HIPAA, CMS Conditions of Participation (CoPs), and professional documentation standards.

Key Principle

Artificial Intelligence should **enhance documentation quality and efficiency—not replace the knowledge, observations, critical thinking, or accountability of the licensed healthcare professional**. The clinician who signs the documentation remains fully responsible for its accuracy, completeness, and compliance with all applicable regulatory and professional standards.

5. Who is ultimately responsible for the accuracy of the medical record?

The **licensed healthcare professional or workforce member who creates, reviews, and signs the documentation** is ultimately responsible for the accuracy, completeness, and integrity of the medical record. Although Artificial Intelligence (AI) may assist with organizing information or drafting documentation, it **cannot assume legal, ethical, or professional responsibility** for the content of the medical record.

Each clinician is accountable for ensuring that documentation:

- Accurately reflects the patient's condition and the services actually provided.
- Is based on the clinician's own assessment, observations, and professional judgment.
- Is complete, objective, timely, and patient-specific.
- Is consistent with the physician's orders, Plan of Care, and agency policies.

- Complies with HIPAA, CMS Conditions of Participation (CoPs), state regulations, accreditation standards, and professional standards of practice.
- Does not contain fabricated, misleading, copied, or unsupported information.

Before signing any documentation, the clinician must carefully review all AI-assisted content, verify its accuracy, correct any errors or omissions, and ensure that it truthfully represents the care delivered. By signing the medical record, the clinician attests that the documentation is accurate and complete.

Supervisors, managers, and agency leadership also share responsibility for promoting documentation quality through education, policy enforcement, quality assurance activities, and ongoing monitoring. However, **the individual who signs the documentation remains personally and professionally accountable for the contents of that record.**

Key Principle

AI is a documentation support tool—it is not responsible for the medical record. The clinician's signature represents professional verification that the documentation is accurate, complete, patient-specific, and compliant with all applicable laws, regulations, and agency policies.

Key Learning Point

Artificial Intelligence may assist with organizing or drafting documentation, but it **must never create clinical findings, patient responses, interventions, or assessments that were not personally observed by the clinician.** Every medical record entry must be accurate, complete, patient-specific, timely, and based on the healthcare professional's own assessment and services provided. The licensed clinician remains fully responsible for the content, accuracy, and integrity of all documentation entered into the patient's medical record.

OASIS Exercises: The Outcome and Assessment Information Set (OASIS) is a standardized patient assessment required by the Centers for Medicare & Medicaid Services (CMS) for Medicare-certified home health agencies. OASIS data supports care planning, quality measurement, reimbursement under the Home Health Patient-Driven Groupings Model (PDGM), public reporting, and quality improvement initiatives.

This training section provides practical exercises to reinforce accurate OASIS completion while emphasizing the appropriate and compliant use of Artificial Intelligence (AI). AI may assist clinicians by organizing information, identifying documentation inconsistencies, or providing educational support; however, AI must never complete, score, or independently determine OASIS responses.

The clinician completing the OASIS assessment remains solely responsible for the accuracy of every response.

Learning Objectives

After completing these exercises, participants should be able to:

- Apply OASIS guidance correctly.
- Use clinical judgment when selecting OASIS responses.
- Recognize situations where AI should not influence OASIS scoring.
- Verify that documentation supports every OASIS response.
- Identify documentation deficiencies that may affect OASIS accuracy.
- Avoid common OASIS coding errors.
- Understand the relationship between OASIS accuracy, patient care, quality measures, and reimbursement.

General Rules

When completing OASIS assessments:

- Base responses on the comprehensive assessment performed during the assessment time point.
- Follow current CMS OASIS Guidance Manual instructions.
- Use physician orders, the patient's medical record, direct observation, patient interview, caregiver interview, and clinical assessment.
- Never guess an answer.
- Never allow AI to choose OASIS responses.
- Document clinical findings that support every selected response.

- If documentation does not support the selected response, revise either the documentation or the OASIS response as appropriate.

Exercise 1 – Medication Review

Scenario

A Start of Care assessment identifies the following medications:

- Aspirin 81 mg daily
- Eliquis 5 mg twice daily
- Hydrocodone/Acetaminophen 5/325 mg as needed
- Metformin 500 mg twice daily

The clinician documents only: "Medication reconciliation completed."

Questions

1. Is this documentation sufficient?
2. What additional documentation is needed?
3. Which high-risk medication categories are represented?

Discussion: The documentation is not sufficient.

The clinician should document:

- Medication review completed.
- Potential interactions identified.
- Duplicate therapies evaluated.
- Physician notification when appropriate.
- Patient education provided.
- Medication compliance assessed.

High-risk medication categories include: Anticoagulant, Hypoglycemic, Opioid

AI may help identify medication classes, but the clinician must verify every medication and document clinical findings independently.

Exercise 2 – Functional Assessment

Scenario: During the comprehensive assessment, the patient walks independently inside the home using a walker. The patient requires standby assistance when climbing stairs.

Question: Should the clinician document the patient as completely independent?

Discussion: No.

The clinician should carefully review the applicable OASIS functional item instructions.

Documentation must accurately reflect the patient's actual functional performance during the assessment period.

AI should never determine the functional response.

Exercise 3 – AI Hallucination

Scenario: An AI documentation tool automatically generates the following statement:

"Patient requires oxygen continuously."

During the visit: No oxygen equipment is present. The physician has not ordered oxygen. The patient denies oxygen use.

Questions: What should the clinician do?

Discussion

The clinician should: Remove the inaccurate statement. Document actual assessment findings. Report recurring AI hallucinations according to agency policy if appropriate.

Never include inaccurate AI-generated information in the medical record.

Exercise 4 – Documentation Support

Scenario: The OASIS indicates the patient is homebound.

The visit note contains no explanation supporting homebound status.

Question: Is this acceptable? Discussion: No.

Documentation must support the OASIS response.

Examples include:

- Requires considerable effort to leave home.
- Uses assistive devices.
- Requires assistance from another person.
- Leaving home is medically contraindicated.
- Limited endurance due to illness.

Without supporting documentation, the OASIS response may be questioned during audits or surveys.

Exercise 5 – Patient-Specific Documentation

Scenario: The clinician copies yesterday's assessment into today's visit note.

Only the date is changed.

Question: Is this acceptable? Discussion: No.

Documentation cloning violates agency policy and may constitute falsification if it does not accurately reflect the current visit.

Every visit must contain individualized documentation based on the clinician's own assessment.

AI-generated summaries must also be individualized.

Exercise 6 – Physician Notification

Scenario: The patient reports increasing shortness of breath and a five-pound weight gain over three days.

The clinician documents the findings but does not notify the physician.

Question: What should occur?

Discussion: The clinician should follow agency policy regarding physician notification for significant changes in condition.

Documentation should include: Clinical findings. Physician notification. New orders received. Patient instructions. Follow-up plan.

AI may identify potential concerns but cannot replace clinical decision-making or physician communication.

Exercise 7 – AI-Assisted Documentation Review

Scenario: AI generates a complete OASIS narrative summarizing the patient's assessment.

Questions: Before signing the documentation, what should the clinician verify?

Discussion: The clinician should verify:

- Patient identity.
- Assessment findings.
- Functional status.
- Medication list.
- Diagnoses.
- Physician orders.
- Skilled services provided.
- Homebound status.
- Patient education.
- Caregiver involvement.
- Consistency between documentation and OASIS responses.

Only after careful review should documentation be finalized.

Common OASIS Errors

Common errors include:

- Unsupported homebound status.
- Incorrect medication documentation.
- Inaccurate functional scoring.
- Missing physician notification.
- Incomplete comprehensive assessment.
- Contradictory documentation.

- AI-generated hallucinations.
- Documentation cloning.
- Failure to individualize patient documentation.
- Unsupported OASIS responses.

Key Learning Points

Participants should remember:

- AI does not complete OASIS assessments.
- AI cannot determine clinical judgment.
- Documentation must support every OASIS response.
- Human oversight is mandatory.
- Every assessment must be individualized.
- Accurate OASIS data supports quality care, regulatory compliance, and appropriate Medicare reimbursement.
- The clinician completing the OASIS assessment is personally responsible for the accuracy, completeness, and integrity of every response entered into the medical record.

Enhanced Topics to Include

We'll also add comprehensive instruction on:

- **AI governance:** AI governance is the framework of policies, procedures, oversight, and accountability that ensures Artificial Intelligence is used safely, ethically, and in compliance with applicable laws and regulations. Its purpose is to protect patients, support healthcare professionals, maintain documentation integrity, and reduce risks associated with AI use.

Key Principles of AI Governance

- AI may only be used for purposes approved by the agency.
- Human oversight is required for all AI-generated content before it is used.
- Licensed healthcare professionals remain responsible for all clinical decisions and documentation.
- Patient privacy and confidentiality must be protected in accordance with HIPAA and agency policies.
- AI-generated information must be verified for accuracy and corrected when necessary.
- The use of AI must comply with CMS Conditions of Participation (CoPs), state regulations, accreditation standards, and agency policies.
- Employees must report suspected AI errors, inappropriate AI use, privacy concerns, or cybersecurity incidents through established agency reporting procedures.

Key Takeaway

Effective AI governance ensures that Artificial Intelligence enhances the quality and efficiency of healthcare services while preserving patient safety, ethical practice, regulatory compliance, and professional accountability.

- **AI ethics:** AI ethics refers to the responsible, fair, and transparent use of Artificial Intelligence in healthcare. Ethical AI ensures that technology supports patient care while protecting patient rights, maintaining professional integrity, and promoting trust in healthcare services. AI should always be used to assist healthcare professionals—not replace their knowledge, clinical judgment, or ethical responsibilities.

Ethical Principles of AI

- **Patient Safety:** AI should only be used in ways that promote safe, high-quality patient care.
- **Human Oversight:** All AI-generated information must be reviewed and verified by a qualified workforce member before use.
- **Accountability:** Healthcare professionals remain responsible for all clinical decisions, documentation, and patient care.
- **Accuracy:** AI-generated information must be verified for correctness before being incorporated into the medical record or used in patient care.
- **Transparency:** Employees should follow agency policies regarding the appropriate use and disclosure of AI in healthcare operations.
- **Privacy and Confidentiality:** Protected Health Information (PHI) must only be used with agency-approved AI systems that comply with HIPAA and applicable privacy regulations.

- **Fairness:** AI should be used without discrimination or bias and should support equitable treatment of all patients.
- **Integrity:** AI must never be used to create false documentation, misrepresent services provided, or conceal errors.

Unethical Uses of AI: Examples of unethical AI use include:

- Creating documentation for services that were not provided.
- Fabricating assessment findings or patient responses.
- Using AI to make independent clinical decisions without professional review.
- Entering patient information into unauthorized AI platforms.
- Using AI to support fraudulent billing, upcoding, or unnecessary services.
- Copying AI-generated documentation into the medical record without verification.

Key Takeaway

Ethical use of Artificial Intelligence requires honesty, accountability, professional judgment, and respect for patient rights. AI is a valuable support tool, but it must always be used responsibly, under human oversight, and in compliance with agency policy, ethical standards, and healthcare regulations.

- **Documentation integrity:** Documentation integrity is the process of ensuring that all information entered into the patient's medical record is accurate, complete, truthful, timely, and patient-specific. The medical record is a legal document that communicates the patient's condition, the care provided, and the clinical decisions made by the healthcare team. While Artificial Intelligence (AI) may assist with drafting or organizing documentation, it must never compromise the integrity of the medical record.

Principles of Documentation Integrity

All clinical documentation should be:

- **Accurate:** Reflect the patient's actual condition and the services provided.
- **Complete:** Include all required assessment findings, interventions, patient responses, education, and follow-up actions.
- **Objective:** Be based on observable facts and measurable clinical findings rather than opinions or assumptions.
- **Timely:** Be completed as soon as possible after the visit in accordance with agency policy.
- **Patient-Specific:** Clearly describe the individual patient's condition and avoid generic or copied statements.
- **Consistent:** Agree with the physician's orders, Plan of Care, medication list, and other clinical documentation.
- **Legible and Professional:** Be easy to read, well organized, and use appropriate medical terminology and approved abbreviations.

AI and Documentation Integrity

AI may be used to assist with:

- Organizing clinical information.
- Improving grammar, spelling, and readability.
- Drafting documentation after the clinician has completed the patient assessment.
- Identifying potential omissions or inconsistencies for clinician review.

AI must **not** be used to:

- Create documentation for visits that did not occur.
- Fabricate assessments, vital signs, interventions, or patient responses.
- Copy generic documentation into multiple patient records.
- Replace the clinician's observations or professional judgment.
- Alter physician orders or clinical findings.

Maintaining Documentation Integrity

Before signing any AI-assisted documentation, employees should:

- Verify that all information is accurate and supported by the patient's assessment.
- Confirm that the documentation reflects the actual services performed.
- Remove or correct any inaccurate, outdated, or fabricated information.

- Ensure that the documentation complies with agency policy, HIPAA, CMS Conditions of Participation (CoPs), and professional standards.
- Report any suspected misuse of AI or documentation irregularities to the appropriate supervisor or compliance representative.

Key Takeaway

Documentation integrity is essential for patient safety, continuity of care, regulatory compliance, quality improvement, and reimbursement. Every healthcare professional is responsible for ensuring that the medical record accurately reflects the care provided. **AI is a documentation support tool, but the clinician remains fully accountable for the accuracy, completeness, and integrity of every entry in the patient's medical record.**

- **Clinical reasoning:** Clinical reasoning is the process by which healthcare professionals collect and analyze patient information, apply their education and experience, make sound clinical judgments, and determine the most appropriate course of care. It is a critical component of safe, effective, and patient-centered home health services. While Artificial Intelligence (AI) can assist by organizing information or providing educational resources, it **cannot replace the clinical reasoning of a qualified healthcare professional.**

Components of Clinical Reasoning

Clinical reasoning involves the ability to:

- Collect accurate patient assessment data.
- Identify actual and potential patient problems.
- Analyze changes in the patient's condition.
- Recognize risks and prioritize patient needs.
- Interpret assessment findings using clinical knowledge and experience.
- Develop appropriate interventions based on physician orders and the Plan of Care.
- Evaluate the patient's response to treatment.
- Modify the care approach when changes in the patient's condition are identified.
- Communicate significant findings to the physician and interdisciplinary team.

AI and Clinical Reasoning

AI may assist healthcare professionals by:

- Organizing clinical information.
- Summarizing medical records or clinical guidelines.
- Identifying potential documentation omissions.
- Providing evidence-based educational resources.
- Supporting quality improvement activities.

However, AI **must not** be used to:

- Diagnose medical conditions.
- Determine the patient's skilled need or homebound status.
- Replace patient assessments.
- Establish or change the Plan of Care.
- Make treatment recommendations without professional review.
- Decide when to notify the physician.
- Replace the clinician's professional judgment or critical thinking.

Professional Responsibility

Licensed healthcare professionals remain responsible for:

- Performing comprehensive patient assessments.
- Applying independent clinical judgment.
- Making safe and appropriate clinical decisions.
- Recognizing changes in the patient's condition.
- Determining when physician notification or emergency intervention is required.
- Ensuring that all clinical decisions are supported by assessment findings, physician orders, agency policy, and accepted standards of practice.

Key Takeaway

Clinical reasoning is a professional skill developed through education, training, experience, and direct patient assessment. Artificial Intelligence can support the clinician by improving efficiency and organizing information, but

it cannot think critically, evaluate a patient's condition, or make clinical decisions. The responsibility for clinical reasoning and patient care always remains with the licensed healthcare professional.

- **Human oversight:** Human oversight is the process of ensuring that a qualified healthcare professional reviews, verifies, and approves all Artificial Intelligence (AI)-generated information before it is used in patient care, clinical documentation, education, billing, or agency operations. Human oversight is essential because AI cannot exercise clinical judgment, evaluate patient conditions, understand the full clinical context, or assume legal or professional responsibility.

Healthcare professionals remain accountable for every decision they make and every document they sign, regardless of whether AI assisted in creating the content.

Why Human Oversight Is Important

Human oversight helps to:

- Protect patient safety.
- Ensure documentation is accurate, complete, and patient-specific.
- Detect AI errors, hallucinations, outdated information, or fabricated content.
- Maintain compliance with HIPAA, CMS Conditions of Participation (CoPs), state regulations, accreditation standards, and agency policies.
- Prevent fraud, waste, and abuse.
- Preserve the integrity of the medical record.
- Support sound clinical decision-making based on professional judgment rather than automated responses.

Responsibilities of the Healthcare Professional

Before using AI-generated information, the healthcare professional should:

- Review all AI-generated content for accuracy and completeness.
- Verify information against the patient's assessment, physician orders, medication list, and Plan of Care.
- Correct any inaccurate, incomplete, or misleading information.
- Ensure documentation reflects the actual care provided and the clinician's own observations.
- Remove any unsupported statements, assumptions, or fabricated information.
- Confirm that no Protected Health Information (PHI) has been disclosed inappropriately.
- Ensure compliance with agency policies and regulatory requirements before finalizing documentation.

AI Cannot Replace Human Oversight

Artificial Intelligence must **not** be relied upon to:

- Perform patient assessments.
- Diagnose medical conditions.
- Interpret clinical findings independently.
- Determine skilled need or homebound status.
- Develop or change the Plan of Care.
- Make treatment decisions.
- Decide when to notify the physician.
- Sign or approve medical documentation.

These responsibilities require professional education, clinical experience, critical thinking, and accountability, all of which remain the responsibility of the licensed healthcare professional.

Consequences of Failing to Provide Human Oversight

Failure to review AI-generated information may result in:

- Patient safety risks.
- Documentation errors or omissions.
- Medication errors.
- HIPAA violations.
- Survey deficiencies.
- Medicare claim denials or repayment requests.
- Fraud, waste, and abuse allegations.
- Disciplinary action by the agency.
- Professional licensure or legal consequences.

Key Takeaway

Human oversight is the foundation of safe and responsible AI use in home health care. AI is a valuable tool that can improve efficiency and support documentation, but **every AI-generated recommendation, document, or clinical statement must be reviewed, validated, and approved by a qualified healthcare professional before it is used. The clinician—not the AI system—is ultimately responsible for patient care, documentation accuracy, and regulatory compliance.**

- **AI limitations:** Artificial Intelligence (AI) is a powerful technology that can improve efficiency, assist with documentation, and support administrative tasks. However, AI has important limitations and should never be considered a substitute for the knowledge, experience, critical thinking, or professional judgment of a qualified healthcare professional. Understanding these limitations helps ensure AI is used safely, ethically, and in compliance with healthcare regulations.

Understanding AI Limitations

AI generates responses by analyzing patterns in large amounts of data. It does not think, reason, understand patient emotions, or exercise professional judgment. AI cannot independently determine what is best for a specific patient or evaluate unique clinical circumstances.

Because AI does not directly observe patients or provide hands-on care, all AI-generated information must be reviewed and verified before use.

What AI Can Do

AI may assist with:

- Drafting administrative documents.
- Organizing and summarizing information.
- Creating educational materials.
- Assisting with policy development.
- Improving grammar and readability.
- Preparing training materials.
- Identifying possible documentation omissions for review.
- Supporting quality improvement activities.

What AI Cannot Do

AI cannot:

- Perform patient assessments.
- Observe physical, emotional, or environmental changes.
- Diagnose illnesses or medical conditions.
- Develop or change a patient's Plan of Care.
- Prescribe medications or treatments.
- Replace nursing, therapy, social work, or physician judgment.
- Determine medical necessity, skilled need, or homebound status.
- Complete OASIS assessments independently.
- Recognize every patient-specific circumstance or clinical nuance.
- Accept legal, ethical, or professional responsibility for patient care.

Risks of Overreliance on AI

Relying on AI without proper human oversight may result in:

- Incorrect or fabricated information (AI hallucinations).
- Inaccurate or incomplete documentation.
- Medication errors.
- Poor clinical decision-making.
- HIPAA violations if confidential information is improperly disclosed.
- Survey deficiencies and regulatory noncompliance.
- Billing errors or allegations of fraud, waste, and abuse.
- Compromised patient safety and quality of care.

Best Practices

To safely use AI in home health care:

- Always verify AI-generated information before using it.

- Compare AI-generated content with the patient's assessment, physician orders, and Plan of Care.
- Use professional judgment to determine whether AI-generated information is appropriate.
- Correct or remove inaccurate, outdated, or unsupported information.
- Follow agency policies regarding AI use, documentation, privacy, and cybersecurity.
- Report concerns about inaccurate AI-generated information or inappropriate AI use to your supervisor or Compliance Officer.

Key Takeaway

Artificial Intelligence is a valuable **support tool**, but it has significant limitations. AI cannot replace clinical reasoning, patient assessment, professional judgment, or ethical decision-making. **The licensed healthcare professional remains fully responsible for all patient care, documentation, and clinical decisions. AI should be used to enhance—not replace—the expertise and accountability of the healthcare workforce.**

- **AI hallucinations:** AI systems generate responses by predicting patterns in data—they do not verify facts or understand clinical situations as a healthcare professional does. As a result, AI may occasionally produce incorrect information that appears believable.

Examples of AI hallucinations include:

- Inventing patient assessment findings.
- Fabricating vital signs or laboratory results.
- Creating medications, dosages, or drug interactions that do not exist.
- Referencing outdated or incorrect clinical guidelines.
- Citing regulations or policies that are inaccurate or nonexistent.
- Generating physician orders or treatment recommendations that were never authorized.
- Adding symptoms, diagnoses, or interventions that were not observed or performed.

Why AI Hallucinations Are Dangerous

If not identified and corrected, AI hallucinations may:

- Compromise patient safety.
- Lead to incorrect clinical decisions.
- Result in medication errors.
- Create inaccurate or fraudulent medical documentation.
- Cause HIPAA or privacy violations.
- Lead to survey deficiencies and regulatory noncompliance.
- Result in denied claims, repayment demands, or allegations of fraud, waste, and abuse.
- Damage patient trust and the agency's professional reputation.

Recognizing AI Hallucinations

Employees should be alert for AI-generated information that:

- Cannot be verified in the patient's medical record.
- Conflicts with the physician's orders or Plan of Care.
- Contains vague, generic, or unsupported statements.
- Includes incorrect medical terminology or clinical recommendations.
- References regulations, standards, or citations that cannot be confirmed.
- Appears inconsistent with the patient's condition or the clinician's assessment.

Preventing AI Hallucinations

To reduce the risk of AI hallucinations:

- Always review and verify AI-generated information before using it.
- Compare AI-generated content with the patient's assessment, physician orders, medication list, and Plan of Care.
- Use current clinical references and agency policies to verify facts.
- Remove or correct inaccurate, unsupported, or fabricated information.
- Never assume AI-generated information is correct simply because it sounds professional.
- Report repeated or significant AI errors through the agency's quality improvement or compliance process.

Professional Responsibility

Artificial Intelligence cannot determine whether the information it generates is accurate for a particular patient. The licensed healthcare professional is responsible for ensuring that all documentation, clinical decisions, and patient care are based on verified facts, professional judgment, and direct patient assessment.

Key Takeaway

AI hallucinations are a recognized limitation of Artificial Intelligence. While AI can be a valuable tool for improving efficiency, **every AI-generated response must be carefully reviewed, verified, and corrected when necessary before it is used in patient care, documentation, education, billing, or agency operations. The clinician—not the AI system—is ultimately responsible for the accuracy and integrity of the information used in healthcare.**

- **Documentation cloning:** Documentation cloning is the practice of copying and reusing the same or substantially similar documentation from one patient, one visit, or one medical record to another without ensuring that it accurately reflects the individual patient's condition and the care actually provided. While Artificial Intelligence (AI) and electronic health record (EHR) systems may assist with drafting or formatting documentation, every medical record entry must be individualized, accurate, and based on the clinician's own assessment and services performed. Documentation cloning can compromise patient safety, reduce the quality of care, and violate Medicare, Medicaid, accreditation, and agency documentation requirements.

What Is Documentation Cloning?

Documentation cloning occurs when:

- The same assessment is copied from a previous visit without verifying the patient's current condition.
- Documentation from one patient is copied into another patient's medical record.
- AI-generated documentation is reused for multiple patients without appropriate individualization.
- Generic statements are repeatedly used without reflecting the patient's actual status.
- Previous documentation is copied forward without updating changes in the patient's condition, medications, or treatment.

Although templates may be used to improve efficiency, each note must be customized to accurately describe the individual patient and the services provided during that specific visit.

Risks of Documentation Cloning

Improper documentation cloning may:

- Create inaccurate or misleading medical records.
- Omit important changes in the patient's condition.
- Result in medication or treatment errors.
- Compromise continuity of care.
- Misrepresent the services actually provided.
- Lead to Medicare claim denials or payment recoupments.
- Result in survey deficiencies during CMS, state, or accreditation surveys.
- Increase the risk of allegations of fraud, waste, or abuse.
- Damage the agency's credibility and professional reputation.

Preventing Documentation Cloning

Healthcare professionals should:

- Perform and document a new assessment during every patient visit.
- Ensure every note reflects the patient's current condition and response to care.
- Update all assessment findings, interventions, medications, and education based on the current visit.
- Remove outdated or irrelevant information before finalizing documentation.
- Review AI-assisted or copied content carefully to confirm that it is accurate, complete, and patient-specific.
- Verify that documentation supports the physician's orders, Plan of Care, and services actually performed.

AI and Documentation Cloning

Artificial Intelligence may assist with organizing documentation or preparing a draft, but it **must never** be used to generate identical clinical notes for multiple patients or to automatically repeat previous documentation without clinician review.

Employees should never use AI to:

- Create duplicate visit notes.
- Copy assessment findings from previous visits without reassessment.

- Generate identical documentation for different patients.
- Replace individualized documentation with generic language.

Key Takeaway

Every patient encounter is unique and must be documented based on the clinician's own assessment, observations, and interventions. **Documentation cloning is not an acceptable documentation practice because it may produce inaccurate medical records and jeopardize patient safety, regulatory compliance, and reimbursement. AI should be used to support documentation efficiency, but every note must be reviewed, individualized, and verified by the clinician before it becomes part of the medical record.**

- **Copy-and-paste risks:** The copy-and-paste function available in electronic health records (EHRs) can improve efficiency when used appropriately; however, improper use may result in inaccurate, outdated, or misleading documentation. When combined with Artificial Intelligence (AI), the risk of copying incorrect or generic information into the medical record increases. Healthcare professionals must ensure that every entry accurately reflects the patient's current condition and the services provided during that specific visit.

Risks of Copy-and-Paste Documentation

Improper use of copy-and-paste may:

- Carry forward outdated or incorrect patient information.
- Create documentation that does not reflect the patient's current condition.
- Duplicate assessment findings that were not verified during the current visit.
- Omit important changes in the patient's health status, medications, or treatment plan.
- Spread documentation errors throughout the medical record.
- Result in inconsistent or contradictory information between visits.
- Reduce the quality and reliability of the medical record.
- Compromise continuity of care among members of the interdisciplinary team.
- Lead to Medicare claim denials or payment recoupments.
- Result in survey deficiencies and increased regulatory scrutiny.
- Increase the risk of allegations of fraud, waste, or abuse if documentation does not accurately reflect the care provided.

Examples of Inappropriate Copy-and-Paste

Examples include:

- Copying a previous assessment without performing a new assessment.
- Reusing wound measurements from a prior visit without remeasuring the wound.
- Copying vital signs from an earlier visit instead of recording current findings.
- Copying patient education without confirming it was provided during the current visit.
- Reusing documentation from one patient in another patient's medical record.
- Copying AI-generated documentation into the medical record without reviewing and verifying its accuracy.

Best Practices

To reduce copy-and-paste risks, employees should:

- Perform and document a complete assessment during every visit.
- Review all copied or AI-assisted text before saving or signing the note.
- Remove outdated, duplicated, or irrelevant information.
- Update all assessment findings, interventions, medications, and patient responses based on the current visit.
- Ensure documentation is accurate, complete, objective, and patient-specific.
- Verify that copied information is supported by the patient's current condition, physician's orders, and Plan of Care.
- Document significant changes in condition rather than repeating prior entries.

AI Considerations

AI may assist with drafting or organizing documentation, but it **must never** be used to automatically copy previous notes or generate repetitive documentation without clinician review. Every AI-assisted note should be carefully reviewed to ensure it reflects the current patient encounter and does not include copied or fabricated information.

Key Takeaway

Copy-and-paste should be used cautiously and only when the information has been carefully reviewed, updated, and verified for the current visit. **Every medical record entry must accurately reflect the patient's current condition, the services actually provided, and the clinician's own assessment. The healthcare professional who signs the documentation remains fully responsible for its accuracy, regardless of whether copied text or AI-assisted content was used.**

- **Upcoding and downcoding:** Accurate clinical documentation is essential to ensure that healthcare services are coded and billed correctly. **Upcoding** and **downcoding** are improper coding practices that can result in inaccurate reimbursement, regulatory violations, and potential legal consequences. Artificial Intelligence (AI) may assist with organizing documentation or identifying coding considerations, but it **must never** be used to increase or decrease the level of service or diagnosis without documentation that fully supports the code assigned. Healthcare professionals are responsible for ensuring that documentation accurately reflects the patient's condition and the services actually provided.

What Is Upcoding?

Upcoding occurs when documentation or coding represents a higher level of service, complexity, or reimbursement than what was actually provided or supported by the medical record.

Examples of upcoding include:

- Documenting a more complex patient condition than was observed.
- Recording services that were not performed.
- Exaggerating the patient's functional limitations or skilled needs.
- Adding diagnoses or complications that are not supported by the assessment or physician documentation.
- Using AI to generate documentation that falsely supports a higher level of reimbursement.

Upcoding may be considered **fraud** and can result in significant penalties.

What Is Downcoding?

Downcoding occurs when documentation or coding reflects a lower level of service or complexity than what was actually provided.

Examples of downcoding include:

- Failing to document all skilled services performed.
- Omitting significant assessment findings.
- Leaving out clinically relevant diagnoses or interventions.
- Incomplete documentation that does not fully support the care delivered.
- Accepting incomplete AI-generated documentation that understates the patient's condition or skilled needs.

Although downcoding may not be intentional, it can lead to underpayment, inaccurate quality reporting, and an incomplete medical record.

Risks of Upcoding and Downcoding

Improper coding practices may result in:

- Incorrect reimbursement.
- Medicare or Medicaid claim denials.
- Repayment of overpayments or underpayments.
- Civil monetary penalties.
- False Claims Act investigations.
- Fraud, waste, and abuse allegations.
- Survey deficiencies.
- Damage to the agency's reputation.
- Disciplinary action or professional licensure consequences.

AI and Coding

Artificial Intelligence may assist by:

- Organizing documentation.
- Identifying documentation gaps for clinician review.
- Summarizing clinical information.
- Supporting education on coding requirements.

AI must not:

- Assign diagnosis or billing codes independently.
- Recommend higher or lower reimbursement without supporting documentation.
- Create documentation solely to justify payment.
- Modify clinical findings to influence reimbursement.
- Replace professional coding or clinical judgment.

Preventing Upcoding and Downcoding

Healthcare professionals should:

- Document only the services actually provided.
- Ensure all diagnoses, interventions, and patient responses are supported by the medical record.
- Verify that coding accurately reflects the documented clinical findings.
- Review AI-assisted documentation for accuracy and completeness before it is finalized.
- Report suspected coding irregularities or inappropriate AI use according to agency policy.

Key Takeaway

Coding and reimbursement must always be supported by **accurate, complete, and truthful clinical documentation**. Neither AI nor any healthcare professional should alter documentation to increase or decrease reimbursement. **The medical record must accurately reflect the patient's condition and the services provided, and the clinician remains responsible for ensuring documentation supports appropriate coding and billing.**

- **False Claims Act:** The **False Claims Act (31 U.S.C. §§ 3729–3733)** is a federal law that protects government healthcare programs, including Medicare and Medicaid, from fraud. The law prohibits knowingly submitting, or causing the submission of, false or fraudulent claims for payment to the federal government. In home health care, accurate documentation is essential because it supports the services billed to Medicare and other federal healthcare programs. Artificial Intelligence (AI) may assist with documentation and administrative tasks, but it **must never** be used to create, alter, or support false claims for reimbursement.

What Is a False Claim?

A false claim occurs when a healthcare provider knowingly submits or causes the submission of a claim that is false, fraudulent, or not supported by the medical record.

Examples include:

- Billing for services that were not provided.
- Documenting patient visits that did not occur.
- Creating or altering documentation after the fact to justify payment.
- Upcoding services to receive higher reimbursement.
- Billing for services that are not medically necessary.
- Falsifying patient assessments, visit times, or clinical findings.
- Submitting claims based on inaccurate or fabricated AI-generated documentation.

AI and the False Claims Act

Improper use of AI may contribute to False Claims Act violations if AI-generated information is accepted without verification or is intentionally used to support inaccurate billing.

Examples include:

- Using AI to create documentation for a visit that never occurred.
- Allowing AI to generate assessment findings that were not observed.
- Using AI-generated documentation to support services that were not medically necessary.
- Copying AI-generated notes into multiple patient records without individualization.
- Failing to correct inaccurate AI-generated documentation before submitting a claim.

Because claims are based on the medical record, **inaccurate documentation can lead to inaccurate billing.**

Employee Responsibilities

All workforce members are responsible for:

- Documenting only the services actually provided.
- Ensuring documentation is truthful, complete, and patient-specific.
- Verifying all AI-assisted documentation before it becomes part of the medical record.
- Reporting suspected fraud, waste, abuse, or false documentation through the agency's compliance reporting process.

- Following agency policies, CMS regulations, and professional standards.

Consequences of False Claims

Violations of the False Claims Act may result in:

- Repayment of Medicare or Medicaid funds.
- Civil monetary penalties.
- Treble (triple) damages as permitted under federal law.
- Exclusion from participation in federal healthcare programs.
- Criminal investigation or prosecution in cases involving intentional fraud.
- Loss of professional licensure.
- Disciplinary action, including termination of employment.
- Damage to the agency's reputation and accreditation status.

Preventing False Claims

Healthcare professionals should:

- Complete and document patient assessments honestly and accurately.
- Never document services that were not performed.
- Never alter documentation to increase reimbursement.
- Carefully review AI-generated documentation for accuracy before signing.
- Ensure all billing is supported by the medical record.
- Report concerns immediately if inaccurate or fraudulent documentation is identified.

Key Takeaway

The False Claims Act requires that **every claim submitted for payment be supported by accurate, complete, and truthful documentation**. Artificial Intelligence should never be used to create or support false documentation or fraudulent claims. **The healthcare professional who documents and signs the medical record is responsible for ensuring that the information is accurate and that any claim submitted is fully supported by the services actually provided.**

- **OIG fraud examples:** The **Office of Inspector General (OIG)** for the U.S. Department of Health and Human Services (HHS) is responsible for identifying, investigating, and preventing fraud, waste, and abuse in federal healthcare programs, including Medicare and Medicaid. The OIG publishes compliance guidance, conducts audits and investigations, and enforces laws designed to protect patients and taxpayer funds.

Home health agencies and their workforce members are expected to comply with all applicable federal regulations and maintain accurate, truthful, and complete documentation. Artificial Intelligence (AI) must never be used in a manner that contributes to fraudulent or abusive practices.

Common OIG Fraud Examples in Home Health

The following are examples of activities that the OIG has identified as potential fraud or abuse when intentionally committed:

- **Billing for services that were not provided.**
- **Creating or signing documentation for visits that never occurred.**
- **Falsifying patient assessments or clinical findings** to justify services or reimbursement.
- **Upcoding** by documenting a higher level of service than was actually provided.
- **Copying and pasting documentation** that does not accurately reflect the current patient encounter.
- **Cloning documentation** across multiple patients or visits without individualization.
- **Billing for services that are not medically necessary.**
- **Submitting claims that are not supported by the medical record.**
- **Altering visit dates, times, or treatment information** after the fact to support billing.
- **Failing to report known overpayments** received from Medicare or Medicaid.
- **Providing or accepting kickbacks, gifts, or incentives** in exchange for patient referrals, which may violate the Federal Anti-Kickback Statute.
- **Using AI to generate false or misleading documentation** that supports billing for services not actually performed.

AI and Fraud Prevention

Artificial Intelligence can improve efficiency, but it must **never** be used to:

- Create documentation for visits that did not occur.

- Invent assessment findings, interventions, or patient responses.
- Generate documentation solely to increase reimbursement.
- Copy the same documentation from one patient to another.
- Replace the clinician's assessment or professional judgment.
- Support billing for services that are not fully documented and medically necessary.

All AI-assisted documentation must be reviewed, verified, and individualized before it becomes part of the patient's medical record.

Red Flags That Should Be Reported

Employees should promptly report concerns such as:

- Documentation that appears identical across multiple patients.
- Records that describe services inconsistent with the patient's condition.
- Billing for services not documented in the medical record.
- Pressure to alter documentation to increase reimbursement.
- Requests to sign documentation for services not personally performed or supervised.
- Suspected misuse of AI to create inaccurate or fabricated documentation.

Reports should be made through the agency's Compliance Officer, supervisor, or other designated reporting process. Employees should report concerns in good faith and in accordance with agency policy.

Consequences of Healthcare Fraud

Fraudulent activities may result in:

- Medicare or Medicaid payment denials and recoupments.
- Civil monetary penalties.
- False Claims Act liability.
- Exclusion from participation in federal healthcare programs.
- Criminal investigation and prosecution.
- Loss of professional licensure or certification.
- Disciplinary action, including termination of employment.
- Damage to the agency's reputation and accreditation status.

Key Takeaway

The OIG expects home health agencies to maintain accurate documentation, bill only for medically necessary services that were actually provided, and operate an effective compliance program to prevent fraud, waste, and abuse. **Every workforce member has a responsibility to document honestly, use AI ethically, report suspected fraud, and help protect the integrity of federal healthcare programs.**

- **Medicare documentation expectations:** Medicare requires that all home health documentation be **accurate, complete, timely, patient-specific, and sufficient to support the medical necessity of services provided.** The medical record serves as the legal record of patient care and is the primary evidence used to determine whether services meet Medicare coverage and payment requirements.

Artificial Intelligence (AI) may assist with organizing information or drafting documentation, but it **cannot replace the clinician's assessment, clinical judgment, or professional responsibility.** Every healthcare professional is responsible for ensuring that documentation accurately reflects the patient's condition and the care actually provided.

Medicare Documentation Principles. Documentation must:

- Be accurate and truthful.
- Reflect the patient's current condition and skilled care needs.
- Support the physician's orders and individualized Plan of Care.
- Demonstrate medical necessity for each service provided.
- Be completed as close to the time of the visit as possible.
- Be legible, complete, dated, timed (when required), and authenticated by the individual providing the service.
- Be individualized for each patient and each visit.
- Support continuity of care among all members of the interdisciplinary team.

Medicare Expects Documentation to Demonstrate

The medical record should clearly show:

- Why the patient qualifies for home health services.
- The patient's clinical condition and current health status.
- The skilled services provided during each visit.
- The patient's response to treatment and interventions.
- Progress toward established goals.
- Changes in the patient's condition.
- Communication with the physician and other members of the care team.
- Patient and caregiver education provided.
- Revisions to the Plan of Care when appropriate.
- Coordination of care among all disciplines involved in the patient's treatment.

Documentation Must Support Medical Necessity

Medicare expects documentation to clearly explain:

- Why skilled nursing, physical therapy, occupational therapy, speech-language pathology, or medical social services are required.
- Why the services must be provided by qualified healthcare professionals.
- How the services are expected to improve, maintain, slow deterioration, or safely manage the patient's condition.
- Why continued home health services remain reasonable and necessary.

Simply stating that a service was performed is **not sufficient**. The documentation should explain the clinical need for the service and the patient's response.

AI and Medicare Documentation

AI may assist with:

- Formatting documentation.
- Organizing clinical information.
- Creating preliminary drafts.
- Identifying documentation gaps for clinician review.
- Assisting with educational materials and administrative tasks.

AI **must not**:

- Complete patient assessments independently.
- Generate visit notes without clinician verification.
- Invent assessment findings, interventions, or patient responses.
- Determine medical necessity.
- Complete OASIS assessments independently.
- Replace the clinician's professional judgment or decision-making.

Every AI-generated entry must be reviewed, corrected as necessary, and approved by the clinician before it becomes part of the medical record.

Common Documentation Deficiencies

Examples of documentation that may not meet Medicare expectations include:

- Generic or repetitive visit notes.
- Copy-and-paste or cloned documentation.
- Missing patient response to treatment.
- Incomplete medication reconciliation.
- Failure to document changes in condition.
- Missing physician notification when required.
- Incomplete patient or caregiver education.
- Documentation that does not support medical necessity.
- Inaccurate or unverified AI-generated documentation.

Best Practices

Healthcare professionals should:

- Perform and document a complete assessment during every visit.
- Document objective clinical findings.
- Record only services actually provided.

- Describe the patient's response to interventions.
- Ensure documentation is consistent throughout the medical record.
- Verify all AI-assisted documentation before signing.
- Complete documentation promptly after the visit.
- Follow agency policies, CMS Conditions of Participation, Medicare billing requirements, and professional standards.

Key Takeaway

Medicare expects every medical record to provide a **clear, accurate, and complete picture of the patient's condition, the skilled services provided, and the medical necessity for those services**. Artificial Intelligence can be a valuable documentation support tool, but **it cannot replace professional assessment, clinical judgment, or documentation responsibility. The clinician who signs the medical record remains fully accountable for its accuracy, completeness, and compliance with Medicare requirements.**

- **Surveyor red flags:** Federal and state surveyors, accreditation organizations, Medicare contractors, and other regulatory agencies evaluate home health agencies to determine whether patient care, documentation, and agency operations comply with applicable laws, regulations, and professional standards. During surveys, reviewers look for "**red flags**"—patterns or deficiencies that may indicate poor documentation, noncompliance, billing errors, fraud, or risks to patient safety.

Understanding these red flags helps employees maintain accurate documentation, support quality patient care, and ensure compliance with the **CMS Conditions of Participation (42 CFR Part 484)**, Medicare requirements, HIPAA, and agency policies.

Common Documentation Red Flags

Surveyors frequently identify concerns such as:

- Identical or nearly identical documentation across multiple patients or visits.
- Copy-and-paste or cloned documentation that does not reflect the current visit.
- Generic statements that lack patient-specific information.
- Missing or incomplete patient assessments.
- Documentation that conflicts with physician orders or the Plan of Care.
- Missing dates, times (when required), signatures, or authentication.
- Late entries that are not properly identified or explained.
- Illegible documentation or unexplained abbreviations.
- Documentation that appears to have been altered after the fact without proper correction procedures.

Clinical Red Flags

Surveyors may identify concerns when documentation shows:

- No evidence of skilled services despite billing for skilled care.
- Failure to document the patient's response to treatment.
- Missing or incomplete medication reconciliation.
- Failure to identify or report significant changes in condition.
- Missing physician notification when required.
- Care that is inconsistent with the patient's diagnosis or physician's orders.
- Lack of measurable progress toward established goals.
- Services that do not appear medically necessary.
- Missing supervisory visits for home health aide services, when applicable.

AI-Related Red Flags

As AI becomes more common in healthcare, surveyors and auditors may pay close attention to documentation that suggests improper AI use, including:

- AI-generated notes that contain fabricated or inaccurate information.
- Documentation that is repetitive, generic, or identical across multiple records.
- Assessment findings that are inconsistent with the patient's condition.
- Clinical recommendations unsupported by the assessment or physician's orders.
- Documentation containing AI hallucinations or factual inaccuracies.
- Notes that appear to have been generated without clinician review or verification.

Billing and Compliance Red Flags

Surveyors and auditors may investigate:

- Billing for services that are not supported by documentation.
- Documentation that appears designed solely to justify reimbursement.
- Upcoding or downcoding.
- Inconsistent visit dates, times, or frequencies.
- Missing documentation supporting homebound status or medical necessity.
- Documentation that does not support OASIS responses or quality reporting.
- Repeated documentation deficiencies identified during internal audits without evidence of corrective action.

Agency Operations Red Flags

Surveyors also evaluate agency systems and may identify concerns such as:

- Staff members who are unfamiliar with agency policies or regulatory requirements.
- Missing competency validations or annual education records.
- Incomplete personnel files or expired licenses and certifications.
- Failure to conduct QAPI activities or implement corrective actions.
- Poor infection prevention practices.
- Inadequate emergency preparedness planning.
- Weak oversight of AI use and documentation practices.

Best Practices to Avoid Red Flags

Employees should:

- Perform and document a complete assessment during every patient visit.
- Individualize documentation for each patient and each encounter.
- Verify all AI-assisted documentation before signing.
- Avoid copy-and-paste and documentation cloning unless the information is reviewed, updated, and appropriate.
- Ensure documentation supports physician orders, the Plan of Care, and medical necessity.
- Complete documentation promptly and accurately.
- Follow agency policies, CMS regulations, HIPAA requirements, and professional standards.
- Report documentation concerns, compliance issues, or suspected misuse of AI through the agency's reporting process.

Key Takeaway

Surveyors look for patterns that indicate documentation inaccuracies, poor clinical practice, or noncompliance with Medicare and regulatory requirements. **Accurate, individualized, timely, and truthful documentation—combined with appropriate human oversight of AI-generated content—is the best way to prevent survey deficiencies and demonstrate high-quality patient care. Every clinician is responsible for ensuring that the medical record accurately reflects the care provided and supports regulatory compliance.**

• **QAPI monitoring:** The **Quality Assessment and Performance Improvement (QAPI)** program is a required component of the **CMS Home Health Conditions of Participation (42 CFR §484.65)**. QAPI is a systematic, data-driven approach used to continuously evaluate, improve, and sustain the quality and safety of patient care, agency operations, and regulatory compliance.

As Artificial Intelligence (AI) becomes integrated into healthcare operations, agencies should incorporate AI-related risks into their QAPI program to ensure that AI technologies are used safely, ethically, and in compliance with federal and state regulations.

Objectives of QAPI Monitoring

The agency's QAPI program is designed to: Improve patient outcomes and quality of care. Identify opportunities for performance improvement. Ensure compliance with CMS Conditions of Participation, Medicare requirements, IPAA, and agency policies. Reduce documentation errors and billing risks. Monitor the safe and appropriate use of AI. Prevent fraud, waste, and abuse. Promote continuous staff education and competency development.

AI-Related QAPI Monitoring

The agency should routinely monitor AI-assisted activities to ensure they meet organizational and regulatory expectations.

Examples of AI performance indicators include:

- Accuracy of AI-assisted documentation.
- Frequency of AI-generated errors or hallucinations.
- Incidents of documentation cloning or excessive copy-and-paste.
- Compliance with human review and approval requirements.
- Appropriate use of AI in accordance with agency policy.
- Staff completion of required AI education and competency validation.
- Privacy and cybersecurity incidents involving AI technologies.
- Reports of suspected misuse or unauthorized AI applications.

Documentation Audits

As part of QAPI, the agency should perform periodic audits of clinical documentation to evaluate:

- Accuracy and completeness.
- Patient-specific documentation.
- Medical necessity.
- Medication reconciliation.
- Compliance with physician orders and the Plan of Care.
- OASIS accuracy and consistency.
- Timeliness of documentation.
- Appropriate authentication and signatures.
- Evidence of clinician review of AI-assisted documentation.

Data Collection and Analysis

The agency should collect and analyze quality data from multiple sources, including:

- Internal chart audits.
- Incident and occurrence reports.
- Patient complaints and grievances.
- Employee reports and compliance concerns.
- Infection prevention data.
- Hospitalizations and emergency department utilization.
- Survey findings.
- Medicare claim denials.
- AI-related documentation issues.
- Patient satisfaction surveys.

Quality data should be reviewed regularly to identify trends, recurring problems, and opportunities for improvement.

Performance Improvement Activities

When deficiencies or trends are identified, the agency should implement Performance Improvement Projects (PIPs) that may include:

- Root cause analysis.
- Corrective action plans.
- Policy revisions.
- Additional staff education.
- Competency validation.
- Increased documentation monitoring.
- Enhanced supervision and coaching.
- Follow-up audits to verify sustained improvement.

Employee Responsibilities

Every workforce member has a role in the QAPI program and is expected to:

- Follow agency policies and procedures.
- Maintain accurate and complete documentation.
- Use AI responsibly and only as authorized.
- Report quality concerns, documentation errors, privacy incidents, and suspected misuse of AI.
- Participate in required education, competency validation, and quality improvement activities.
- Cooperate with internal audits and corrective action initiatives.

Leadership Responsibilities

Agency leadership, including the Governing Body, Administrator, Clinical Manager, Director of Nursing, Compliance Officer, Privacy Officer, and QAPI Committee, is responsible for:

- Providing oversight of the QAPI program.
- Monitoring compliance with regulatory requirements.
- Reviewing quality indicators and audit results.
- Evaluating AI-related risks and mitigation strategies.
- Allocating resources to support performance improvement.
- Ensuring corrective actions are implemented, monitored, and sustained.
- Promoting a culture of patient safety, ethical practice, and continuous quality improvement.

Key Performance Indicators (KPIs)

Examples of QAPI indicators that may be monitored include:

- Documentation accuracy rate.
- OASIS accuracy rate.
- Medication reconciliation compliance.
- Timely completion of visit documentation.
- Home health aide supervisory visit compliance.
- Physician notification compliance.
- Patient satisfaction scores.
- Hospital readmission rates.
- Infection prevention compliance.
- AI documentation error rate.
- AI competency completion rate.
- Number of reported AI-related incidents or privacy concerns.

Key Takeaway

An effective QAPI program continuously monitors the quality, safety, and compliance of patient care while supporting organizational improvement. **AI should be included in the agency's QAPI activities to ensure it is used responsibly, accurately, and ethically. Continuous monitoring, auditing, education, and corrective action help protect patients, support regulatory compliance, and promote high-quality home health services.**

- **Incident investigations:** Incident investigations are a critical component of the agency's Quality Assessment and Performance Improvement (QAPI) and Compliance Programs. Their purpose is to identify the cause of an incident, determine whether patient safety or regulatory compliance was affected, implement corrective actions, and prevent recurrence.

Incidents involving the use of **Artificial Intelligence (AI)** require the same level of review as any other clinical or operational event. AI-assisted documentation or recommendations do not eliminate the responsibility of healthcare professionals to provide safe, accurate, and compliant patient care.

What Is an Incident?

An incident is any unexpected event, error, omission, or circumstance that has the potential to affect: Patient safety. Quality of care. Documentation accuracy. Privacy or confidentiality. Regulatory compliance. Agency operations. Billing integrity. Cybersecurity.

Incidents may result in actual harm, have the potential to cause harm (near misses), or reveal weaknesses in agency processes that require corrective action.

Examples of Incidents

Examples include: Medication errors. Patient falls or injuries. Incorrect or delayed treatment. Documentation errors or omissions. Copy-and-paste or documentation cloning identified in the medical record. AI-generated hallucinations incorporated into documentation. Unauthorized disclosure of Protected Health Information (PHI). Cybersecurity incidents involving AI or electronic health records. Billing or coding errors. Failure to notify the physician of a significant change in condition. Use of an unauthorized AI application to process patient information. Submission of inaccurate documentation that could affect reimbursement.

Reporting Responsibilities: All workforce members are responsible for promptly reporting incidents according to agency policy. Reports should be made **immediately or as soon as reasonably possible** after the incident is discovered and should include factual, objective information.

Employees should never attempt to conceal, alter, or destroy documentation related to an incident.

Investigation Process

Incident investigations generally include the following steps:

1. **Ensure Immediate Safety**
 - Protect the patient, staff, and others from further harm.
 - Provide any necessary clinical intervention.
2. **Notify Appropriate Personnel**
 - Inform the supervisor, Clinical Manager, Administrator, Compliance Officer, Privacy Officer, or other designated leadership as required.
3. **Secure Relevant Information**
 - Preserve documentation, electronic records, physician orders, AI-generated content (if applicable), audit logs, and other relevant evidence.
4. **Conduct a Thorough Review**
 - Review the medical record.
 - Interview involved personnel when appropriate.
 - Determine what occurred, when it occurred, and why it occurred.
 - Identify whether AI contributed to the incident.
5. **Perform Root Cause Analysis**
 - Identify the underlying system, process, training, technology, or human factors that contributed to the event.
 - Focus on improving processes rather than assigning blame whenever appropriate.
6. **Develop Corrective Actions**
 - Revise policies or procedures.
 - Provide additional education or competency validation.
 - Improve documentation practices.
 - Strengthen AI oversight and approval processes.
 - Implement additional monitoring when necessary.
7. **Monitor Effectiveness**
 - Follow up through QAPI audits and performance monitoring to ensure corrective actions are effective and sustained.

AI-Related Incident Investigations

When AI is involved, investigators should determine:

- Whether AI-generated information was reviewed by the clinician.
- Whether inaccurate or fabricated information (AI hallucinations) was included in the medical record.
- Whether documentation cloning or excessive copy-and-paste occurred.
- Whether Protected Health Information (PHI) was entered into an unauthorized AI platform.
- Whether AI contributed to an incorrect clinical decision or documentation error.
- Whether agency AI policies and procedures were followed.
- Whether additional staff education or system improvements are needed.

Documentation of the Investigation

Investigation records should be: Accurate and objective. Based on verified facts rather than assumptions.

Completed promptly. Maintained in accordance with agency policy and applicable legal requirements. Shared only with individuals who have a legitimate business or regulatory need to know. Incident investigation documentation should **never** be altered to minimize or conceal an event.

Employee Responsibilities.

All workforce members are expected to:

- Report incidents promptly.
- Cooperate fully with investigations.
- Provide truthful and complete information.

- Preserve documentation and evidence.
- Participate in corrective actions and additional education when required.
- Follow updated policies and procedures developed as a result of the investigation.

Key Takeaway

Incident investigations are essential for protecting patients, maintaining regulatory compliance, and improving the quality of care. **Every incident—including those involving AI—should be reported, investigated, documented, and analyzed to identify root causes and implement effective corrective actions. A culture of transparency, accountability, and continuous improvement helps prevent recurrence and strengthens patient safety.**

• **Root Cause Analysis:** Root Cause Analysis (RCA) is a structured, systematic process used to identify the underlying causes of an incident, error, near miss, or performance problem rather than simply addressing its immediate effects. Within a home health agency, Root Cause Analysis is an essential component of the **Quality Assessment and Performance Improvement (QAPI) Program**, helping the organization improve patient safety, strengthen regulatory compliance, and prevent similar events from occurring in the future.

When Artificial Intelligence (AI) is involved in an incident, the investigation should determine whether AI contributed to the event and whether appropriate human oversight and verification were performed.

What Is Root Cause Analysis? Root Cause Analysis is a method of answering the question:

"Why did this happen?" Instead of assigning blame to an individual, RCA focuses on identifying weaknesses in systems, processes, communication, education, technology, or organizational practices that allowed the event to occur. The goal is to implement lasting improvements that reduce the likelihood of recurrence.

When Should Root Cause Analysis Be Performed? The agency should consider performing an RCA for events such as:

- Patient injuries or unexpected adverse events.
- Medication errors.
- Significant documentation deficiencies.
- Privacy or HIPAA breaches.
- Cybersecurity incidents.
- Incorrect OASIS assessments affecting patient care or reimbursement.
- Billing or coding errors.
- Survey deficiencies or repeat citations.
- AI-generated hallucinations incorporated into the medical record.
- Documentation cloning or inappropriate copy-and-paste practices.
- Suspected fraud, waste, or abuse.
- Near misses with the potential to cause patient harm.

The Root Cause Analysis Process. A structured RCA generally includes the following steps:

1. Define the Problem

Clearly identify: What happened. When it occurred. Who was involved. How the event was discovered. The actual or potential impact on patient care, compliance, or agency operations.

2. Gather the Facts

Collect all relevant information, including: Patient records. Physician orders. Visit notes. OASIS assessments. Medication records. Incident reports. AI-generated content (if applicable). Audit logs. Staff interviews. Applicable agency policies and procedures.

The investigation should rely on objective evidence rather than assumptions.

3. Identify Contributing Factors

Determine what conditions contributed to the event, such as: Inadequate education or competency. Poor communication. Incomplete documentation. Failure to follow agency policy. Technology or software issues. Workflow inefficiencies. Insufficient supervision. Human error. Improper use of AI.

Most incidents involve multiple contributing factors rather than a single mistake.

4. Determine the Root Cause

Examples of root causes may include:

- Inadequate staff training.
- Lack of policy awareness.
- Weak documentation processes.

- Insufficient quality monitoring.
- Poor communication between disciplines.
- Failure to verify AI-generated information.
- Inadequate cybersecurity controls.
- Deficient oversight by leadership.
- Ineffective workflows or system design.

The objective is to identify **why** the problem occurred—not simply **who** made the error.

AI-Specific Root Cause Analysis

When AI contributes to an event, investigators should determine:

- Was AI approved for the intended purpose?
- Did the clinician independently verify the AI-generated information?
- Were AI hallucinations identified before documentation was finalized?
- Was patient-specific information accurately reflected?
- Did documentation cloning or excessive copy-and-paste occur?
- Was Protected Health Information entered into an unauthorized AI application?
- Were agency AI policies followed?
- Was additional education or supervision needed?

Developing Corrective Actions

After identifying the root cause, the agency should implement corrective actions that address the underlying problem rather than only the immediate error.

Corrective actions may include:

- Revising policies and procedures.
- Providing additional education and competency validation.
- Improving documentation standards.
- Enhancing supervision and clinical oversight.
- Strengthening AI governance and approval processes.
- Implementing additional quality audits.
- Improving cybersecurity safeguards.
- Updating electronic health record workflows.
- Increasing QAPI monitoring.

Corrective actions should be realistic, measurable, and sustainable.

Monitoring Effectiveness

Corrective actions should be monitored through the QAPI program to determine whether they successfully prevent recurrence. Monitoring may include:

- Follow-up chart audits.
- Documentation reviews.
- AI usage audits.
- Competency assessments.
- Incident trend analysis.
- Survey readiness reviews.
- Patient outcome monitoring.
- Compliance reports.

If the problem persists, additional corrective actions should be implemented.

Employee Responsibilities

All workforce members are expected to:

- Report incidents promptly.
- Participate honestly in investigations.
- Provide accurate information.
- Cooperate with Root Cause Analysis activities.
- Participate in additional education when required.
- Follow revised policies and procedures.
- Support continuous quality improvement.

Leadership Responsibilities

Agency leadership is responsible for:

- Ensuring Root Cause Analyses are conducted objectively.
- Promoting a non-punitive culture that encourages reporting and learning.
- Providing resources to implement corrective actions.
- Monitoring long-term effectiveness of improvements.
- Reporting significant findings through the QAPI Committee and Governing Body when appropriate.
- Ensuring AI-related risks are incorporated into the agency's quality improvement program.

Key Takeaway

Root Cause Analysis is a proactive quality improvement tool that helps the agency understand **why** incidents occur and how to prevent them from happening again. **Rather than focusing on individual blame, RCA examines systems, processes, education, technology, communication, and human factors to identify sustainable solutions. As AI becomes increasingly integrated into healthcare, agencies must include AI-related events in their Root Cause Analysis process to ensure patient safety, regulatory compliance, and continuous quality improvement.**

- **Vendor management:** Vendor management is the process used by the agency to evaluate, approve, monitor, and oversee outside companies that provide technology, software, equipment, consulting, data processing, cloud storage, Artificial Intelligence (AI), or other services. Effective vendor management is essential because third-party vendors may have access to agency systems, confidential business information, Protected Health Information (PHI), or clinical workflows. The agency remains responsible for protecting patient information and ensuring that vendor services support safe, compliant, and reliable operations.

Types of Vendors That May Require Oversight

Examples include:

- Electronic health record vendors.
- AI software providers.
- Billing and coding companies.
- Cloud storage providers.
- Cybersecurity vendors.
- Telehealth and remote monitoring companies.
- Payroll and human resources platforms.
- Medical equipment suppliers.
- Consultants and contractors.
- Document storage and destruction companies.
- Communication and messaging platforms.

Pre-Approval Evaluation

Before entering into an agreement, the agency should evaluate whether the vendor:

- Has appropriate experience in healthcare.
- Can meet the agency's operational and compliance needs.
- Maintains adequate privacy and cybersecurity safeguards.
- Complies with HIPAA and other applicable laws.
- Has a process for identifying and reporting security incidents.
- Provides reliable technical support.
- Maintains appropriate insurance coverage.
- Uses subcontractors and, if so, how those subcontractors are monitored.
- Can preserve, return, or securely destroy agency data when the contract ends.

For AI vendors, the agency should also evaluate:

- The intended use of the AI system.
- The type of information used to generate outputs.
- Whether PHI will be entered, stored, or processed.
- How the system protects confidential data.
- Whether submitted data is used to train the vendor's models.

- How AI-generated information is validated.
- Known limitations, error rates, or risks.
- Whether human review is required before use.
- Whether the agency can access audit logs or usage reports.

Business Associate Agreements

When a vendor creates, receives, maintains, or transmits PHI on behalf of the agency, the agency should determine whether a **Business Associate Agreement (BAA)** is required.

The BAA should address:

- Permitted uses and disclosures of PHI.
- Required privacy and security safeguards.
- Breach and incident reporting.
- Use of subcontractors.
- Return or destruction of PHI.
- Compliance with applicable HIPAA requirements.

A BAA does not eliminate the agency's responsibility to evaluate and monitor the vendor.

Contract Requirements

Vendor contracts should clearly define:

- The services to be provided.
- Performance expectations.
- Privacy and confidentiality obligations.
- Data ownership.
- Data storage locations.
- Cybersecurity requirements.
- Incident reporting timeframes.
- Access controls.
- Audit rights.
- Service interruption procedures.
- Data backup and recovery.
- Contract termination responsibilities.
- Return, transfer, or destruction of agency information.

For AI vendors, contracts should also address:

- Approved uses of the AI system.
- Prohibited uses.
- Restrictions on using agency or patient data for model training.
- Human oversight requirements.
- Responsibility for inaccurate or harmful outputs.
- System updates or material changes.
- Monitoring and reporting capabilities.

Ongoing Vendor Monitoring

Approved vendors should be monitored based on the level of risk associated with their services.

Monitoring may include:

- Reviewing performance reports.
- Evaluating service quality.
- Reviewing security certifications or assessments.
- Monitoring system availability and downtime.
- Reviewing complaints and incident reports.
- Confirming continued compliance with contract requirements.
- Reviewing AI-generated error trends.
- Monitoring unauthorized access or inappropriate use.
- Reassessing vendors when services or risks change.

High-risk vendors should receive more frequent review.

AI Vendor Red Flags. Potential warning signs include:

- The vendor cannot clearly explain how patient data is used.
- The platform does not offer a BAA when one is required.
- Data may be used to train public or shared AI models.
- The system produces frequent inaccurate or fabricated information.
- The vendor does not provide adequate access controls.
- The vendor cannot provide audit logs.
- Security incidents are not reported promptly.
- The system encourages users to rely on AI without human verification.
- Contract terms allow broad use or ownership of agency data.
- The vendor makes unsupported claims regarding regulatory compliance.

Vendor Access Controls

Vendor access to agency systems should be limited to the minimum necessary information and functions required to perform the contracted service.

The agency should:

- Approve access before it is granted.
- Use unique user credentials.
- Apply role-based access.
- Require multifactor authentication when appropriate.
- Monitor vendor activity.
- Remove access promptly when it is no longer needed.
- Periodically verify that access remains appropriate.

Vendor Incidents

If a vendor experiences a privacy, security, operational, or AI-related incident, the agency should:

- Obtain immediate information about the event.
- Determine what systems and data were affected.
- Protect patients and agency operations.
- Notify leadership and designated privacy, security, or compliance personnel.
- Preserve relevant evidence.
- Follow breach assessment and reporting requirements.
- Conduct or participate in a Root Cause Analysis.
- Implement corrective actions.
- Reevaluate whether continued use of the vendor is appropriate.

Termination of a Vendor Relationship

When a vendor relationship ends, the agency should ensure:

- Vendor access is disabled.
- Agency data is returned, transferred, or securely destroyed.
- Equipment and credentials are recovered.
- Outstanding incidents or obligations are resolved.
- Records are retained according to law and agency policy.
- Replacement services are implemented without disrupting patient care.

Employee Responsibilities

Employees should:

- Use only agency-approved vendors and applications.
- Never enter PHI into an unapproved AI or software platform.
- Follow agency access and security procedures.
- Report vendor performance problems or suspicious activity.
- Notify leadership if a vendor requests information beyond what is necessary.
- Verify AI-generated information before it is used in patient care, documentation, or operations.

Leadership Responsibilities

Agency leadership is responsible for:

- Establishing a vendor approval process.
- Assigning responsibility for vendor oversight.

- Evaluating vendor risk.
- Ensuring required contracts and BAAs are in place.
- Monitoring vendor performance and compliance.
- Including high-risk vendors in QAPI, privacy, and cybersecurity monitoring.
- Taking corrective action when vendor performance creates risk.

Key Takeaway

Vendors can improve agency efficiency and access to technology, but they may also create privacy, cybersecurity, operational, and clinical risks. **The agency must carefully evaluate vendors before approval, establish clear contractual protections, monitor ongoing performance, and ensure that AI vendors are used only for authorized purposes with appropriate human oversight. The agency remains responsible for protecting patient information and maintaining compliance, even when services are performed by a third party.**

- **Data ownership:** Data ownership establishes who has the legal authority and responsibility for the information created, collected, maintained, and used by the home health agency. In healthcare, patient information is one of the agency's most valuable assets and must be managed in accordance with **HIPAA**, the **CMS Conditions of Participation (42 CFR Part 484)**, state laws, and agency policies.

As Artificial Intelligence (AI) becomes increasingly integrated into healthcare, employees must understand that using AI does **not** transfer ownership of agency or patient data to the AI vendor or software provider. The agency remains responsible for protecting the confidentiality, integrity, and availability of all patient and business information.

What Is Agency Data?

Agency data includes, but is not limited to:

- Patient medical records.
- Protected Health Information (PHI).
- OASIS assessments.
- Plans of Care.
- Physician orders.
- Visit documentation.
- Medication records.
- Billing and reimbursement information.
- Employee records.
- Financial records.
- Quality improvement and QAPI data.
- Policies and procedures.
- Training materials.
- Business reports and operational information.

This information belongs to the agency or is maintained by the agency on behalf of its patients and must be protected throughout its lifecycle.

Data Ownership Principles

The agency is responsible for ensuring that:

- Patient information is collected and used only for authorized purposes.
- Data remains accurate, complete, and secure.
- Access is limited to authorized workforce members.
- Information is protected from unauthorized disclosure, alteration, or destruction.
- Records are retained and disposed of according to legal and regulatory requirements.
- Third-party vendors comply with contractual and privacy obligations.

Employees are custodians of agency information and are responsible for safeguarding the data entrusted to them.

AI and Data Ownership

When AI is used within the agency:

- The agency retains ownership of all patient and business data entered into approved AI systems.
- Employees should use only agency-approved AI applications.
- Patient information must never be entered into unauthorized public AI platforms.

- AI vendors should not obtain ownership of agency data through their terms of service or contractual agreements.
- AI-generated outputs become part of the agency's records only after review, verification, and acceptance by authorized personnel.
- Any AI-generated documentation included in the medical record remains subject to the same legal, regulatory, and documentation requirements as any other clinical documentation.

Protecting Agency Data

To safeguard agency information, employees should:

- Access only the information necessary to perform assigned duties.
- Protect usernames, passwords, and authentication credentials.
- Log out of systems when work is complete.
- Use encrypted and agency-approved devices whenever possible.
- Follow agency policies regarding electronic communication and data storage.
- Immediately report suspected privacy breaches or cybersecurity incidents.
- Verify that AI-generated content does not disclose confidential information to unauthorized individuals.

Vendor Responsibilities

When third-party vendors process agency information, they should:

- Protect data using appropriate administrative, physical, and technical safeguards.
- Comply with HIPAA and applicable privacy laws.
- Execute a Business Associate Agreement (BAA) when required.
- Limit access to authorized personnel.
- Report security incidents promptly.
- Return or securely destroy agency data upon termination of the agreement, as required by the contract and applicable law.
- Refrain from using agency or patient data for unauthorized purposes, including training AI models, unless specifically authorized by contract and permitted by law.

Data Retention and Disposal

Agency data should be:

- Maintained according to federal and state record retention requirements.
- Protected from unauthorized alteration or deletion.
- Archived securely when appropriate.
- Destroyed using secure methods when retention periods expire and destruction is permitted by law and agency policy.

Employees should never delete, alter, or remove agency records without authorization.

Employee Responsibilities

Every workforce member is responsible for:

- Protecting patient and agency information.
- Using data only for legitimate business and patient care purposes.
- Following agency privacy and security policies.
- Reporting unauthorized access or disclosure immediately.
- Using only approved AI technologies.
- Verifying AI-generated information before it is incorporated into agency records.
- Respecting patient confidentiality at all times.

Leadership Responsibilities

Agency leadership is responsible for:

- Establishing policies governing data ownership and data governance.
- Approving technologies that access or process agency information.
- Ensuring contracts clearly define data ownership rights.
- Monitoring compliance with privacy and security requirements.
- Conducting periodic audits of data access and AI usage.
- Responding promptly to data breaches or security incidents.
- Ensuring compliance with HIPAA, CMS Conditions of Participation, and applicable state laws.

Key Takeaway

Patient information and agency business records are valuable assets that must be protected throughout their entire lifecycle. **The agency retains ownership and responsibility for its data even when third-party vendors or AI technologies are used. Every workforce member shares responsibility for safeguarding confidential information, using only approved technologies, and ensuring that all data is handled securely, ethically, and in compliance with federal and state regulations.**

- **Explainable AI:** Explainable Artificial Intelligence (Explainable AI or XAI) refers to AI systems that provide understandable, transparent, and interpretable information about how they generate recommendations, summaries, predictions, or other outputs. In healthcare, explainability is essential because clinicians must understand and verify AI-generated information before using it to support patient care, documentation, quality improvement, or operational decisions.

Explainable AI promotes **patient safety, regulatory compliance, ethical decision-making, and accountability** by helping healthcare professionals understand the basis for AI-generated results rather than accepting them without question.

What Is Explainable AI?

Explainable AI is the ability of an AI system to:

- Describe how it reached a conclusion or recommendation.
- Identify the information used to generate an output.
- Explain the reasoning or factors that influenced its response.
- Allow users to evaluate whether the information is appropriate for the specific clinical situation.
- Support informed human decision-making rather than replacing it.

Not all AI systems provide the same level of transparency. Some AI models produce outputs without clearly explaining how those conclusions were reached. This is sometimes referred to as a **"black box"** system.

Why Explainability Matters in Healthcare

Healthcare decisions can directly affect patient safety, treatment outcomes, reimbursement, and regulatory compliance. Clinicians must be able to evaluate whether AI-generated information is: Accurate. Complete. Current. Supported by clinical evidence. Consistent with physician orders and the Plan of Care. Appropriate for the individual patient's condition.

Without explainability, healthcare professionals may find it difficult to identify errors, inaccuracies, or AI hallucinations.

Benefits of Explainable AI

Explainable AI can help:

- Increase clinician confidence in AI-assisted tools.
- Improve patient safety by supporting verification of AI-generated information.
- Facilitate better clinical decision-making.
- Reduce documentation errors.
- Support regulatory compliance and audit readiness.
- Improve quality improvement and QAPI activities.
- Enhance accountability and transparency.
- Promote responsible and ethical AI use.

Limitations of Explainable AI

Even when AI provides an explanation, employees should understand that:

- AI explanations may still contain errors.
- AI may rely on incomplete or outdated information.
- AI cannot independently determine what is clinically appropriate for a specific patient.
- AI cannot replace professional judgment, experience, or direct patient assessment.
- Explainability does not guarantee that the AI output is correct.

Every AI-generated recommendation must still be independently reviewed and verified.

Human Oversight

Healthcare professionals must:

- Review AI-generated information critically.
- Understand the basis of AI recommendations whenever possible.

- Compare AI output with the patient's assessment, physician's orders, Plan of Care, and current clinical evidence.
- Question AI recommendations that appear inconsistent or unsupported.
- Correct or discard inaccurate AI-generated information.
- Never rely solely on AI when making clinical or operational decisions.

Explainable AI and Documentation

When AI assists with documentation:

- Clinicians should understand how AI generated summaries or suggested content.
- Documentation should accurately reflect the clinician's own assessment and services performed.
- AI-generated documentation must be individualized for each patient.
- The clinician should be able to explain and defend every statement contained in the medical record.
- Documentation should never contain information that cannot be verified.

If a clinician cannot explain or verify AI-generated content, it should **not** be included in the patient's medical record.

Employee Responsibilities

Every workforce member should:

- Use only agency-approved AI systems.
- Verify all AI-generated information before use.
- Understand that AI recommendations are advisory and not authoritative.
- Report AI outputs that appear inaccurate, biased, misleading, or unsafe.
- Follow agency policies governing AI use, documentation, privacy, and cybersecurity.
- Maintain accountability for all work products created with AI assistance.

Leadership Responsibilities

Agency leadership should:

- Select AI technologies that support transparency whenever practical.
- Evaluate AI systems before implementation.
- Educate employees about AI capabilities and limitations.
- Establish policies requiring human review of AI-generated outputs.
- Monitor AI performance through the QAPI program.
- Investigate AI-related incidents and implement corrective actions when needed.

Key Takeaway

Explainable AI helps healthcare professionals understand **how and why** an AI system generated a recommendation or response. However, **explainability does not eliminate the need for human oversight**. Every clinician remains responsible for independently verifying AI-generated information, exercising professional judgment, and ensuring that all documentation, patient care, and operational decisions are accurate, ethical, and compliant with applicable laws and regulations.

• **Bias mitigation:** Bias mitigation is the process of identifying, reducing, and preventing unfair or inappropriate bias in Artificial Intelligence (AI) systems and in human decision-making. In healthcare, bias can negatively affect patient care, clinical decisions, documentation, resource allocation, and access to services. The home health agency is committed to providing equitable, patient-centered care and using AI in a manner that promotes fairness, accuracy, transparency, and compliance with federal and state laws. AI should support clinical decision-making without introducing or reinforcing discrimination or unequal treatment.

What Is AI Bias?

AI bias occurs when an AI system produces outputs or recommendations that are unfair, inaccurate, or systematically favor or disadvantage certain individuals or groups because of limitations in the data, algorithms, or design of the system.

Bias may result from:

- Incomplete or unrepresentative training data.
- Historical healthcare disparities reflected in data.
- Incorrect assumptions within AI models.
- Poor system design.
- Human bias introduced during development or implementation.

- Misinterpretation of AI-generated information.

Bias can occur even when there is no intent to discriminate.

Examples of Bias in Healthcare

Examples include:

- Recommending different levels of care for similar patients without clinical justification.
- Producing inaccurate documentation for certain patient populations.
- Misinterpreting symptoms because of incomplete or biased training data.
- Generating educational materials that are not culturally or linguistically appropriate.
- Producing recommendations that overlook patients with disabilities, limited English proficiency, or unique healthcare needs.
- Suggesting care plans that are inconsistent with current clinical evidence or physician orders.

Why Bias Matters

Bias in AI may:

- Compromise patient safety.
- Contribute to healthcare disparities.
- Affect clinical decision-making.
- Reduce patient trust.
- Produce inaccurate documentation.
- Create ethical and legal concerns.
- Increase regulatory and compliance risks.
- Negatively affect quality outcomes and patient satisfaction.

Healthcare professionals must recognize that AI recommendations should always be evaluated for fairness and appropriateness before they are used.

Strategies to Mitigate Bias

The agency should implement practices that help reduce AI bias, including:

- Using only agency-approved AI technologies.
- Selecting AI systems that are regularly evaluated for accuracy and fairness.
- Requiring human review of all AI-generated clinical information.
- Comparing AI recommendations with current clinical guidelines and evidence-based practice.
- Ensuring documentation accurately reflects the individual patient's condition.
- Providing ongoing education regarding AI limitations and bias awareness.
- Monitoring AI performance through the QAPI program.
- Investigating reports of biased or inaccurate AI outputs.
- Updating policies and procedures as AI technologies evolve.

Human Oversight

Healthcare professionals should:

- Evaluate every AI recommendation using professional judgment.
- Consider the patient's individual clinical condition, goals, culture, language, preferences, and circumstances.
- Avoid relying solely on AI when making patient care decisions.
- Question AI outputs that appear inconsistent, discriminatory, or unsupported by clinical evidence.
- Correct or disregard AI-generated information that is inaccurate or unfair.
- Document care based on objective assessment findings rather than AI assumptions.

Employee Responsibilities

Every workforce member should:

- Treat all patients fairly, respectfully, and without discrimination.
- Use AI only as a decision-support tool.
- Verify AI-generated information before incorporating it into documentation or patient care.
- Report suspected biased AI outputs through the agency's quality improvement or compliance reporting process.
- Participate in required education on AI ethics, bias, and responsible AI use.
- Follow agency policies governing nondiscrimination, patient rights, and AI use.

Leadership Responsibilities

Agency leadership should:

- Evaluate AI technologies before implementation.
- Consider fairness, transparency, and explainability during vendor selection.
- Establish policies requiring human oversight of AI-assisted activities.
- Monitor AI performance for evidence of bias through QAPI audits and incident reporting.
- Investigate complaints involving potential AI bias.
- Provide education and competency validation on bias recognition and mitigation.
- Promote a culture of equity, inclusion, and patient-centered care.

Regulatory and Ethical Considerations

Bias mitigation supports compliance with:

- CMS Conditions of Participation (42 CFR Part 484).
- HIPAA Privacy and Security Rules.
- Federal civil rights and nondiscrimination requirements.
- Agency policies on patient rights and equal access to care.
- Ethical principles of fairness, respect, accountability, and patient-centered care.

While AI can assist healthcare professionals, it must never be used in a manner that results in unequal treatment or discrimination.

Key Takeaway

Bias mitigation is an essential component of responsible AI use in healthcare. **Artificial Intelligence should enhance—not compromise—fair, equitable, and patient-centered care. Every workforce member is responsible for recognizing the potential for AI bias, independently evaluating AI-generated information, and ensuring that all clinical decisions and documentation are based on objective assessment findings, professional judgment, and the individual needs of each patient.**

- **Patient communication:** Effective patient communication is essential to providing safe, high-quality, patient-centered home health care. Clear, respectful, and compassionate communication helps patients and caregivers understand their health conditions, treatment plans, medications, and responsibilities while promoting trust and informed decision-making.

Artificial Intelligence (AI) may assist healthcare professionals in developing educational materials, translating information, or preparing communication drafts. However, **AI must never replace direct communication, clinical judgment, or the therapeutic relationship between healthcare professionals and patients.**

Principles of Effective Patient Communication

Healthcare professionals should communicate in a manner that is:

- Respectful and compassionate.
- Honest and accurate.
- Clear and easy to understand.
- Patient-centered and culturally sensitive.
- Appropriate to the patient's health literacy and preferred language.
- Timely and responsive.
- Consistent with physician orders and the Plan of Care.
- Supportive of patient rights and informed decision-making.

AI-Assisted Patient Communication

AI may be used to assist with:

- Creating patient education materials.
- Simplifying complex medical information.
- Translating educational content into other languages.
- Drafting non-clinical communications for clinician review.
- Developing general health education resources.

All AI-generated communications must be reviewed by qualified staff to ensure they are:

- Accurate.
- Current.
- Appropriate for the individual patient.

- Consistent with the physician's orders and Plan of Care.
- Free of misleading or fabricated information.

AI Should Not Replace Human Communication

Healthcare professionals should **never** rely on AI to:

- Deliver diagnoses or prognoses directly to patients.
- Explain individualized treatment recommendations without clinician involvement.
- Answer complex clinical questions independently.
- Obtain informed consent.
- Resolve patient complaints or grievances without appropriate staff involvement.
- Provide emotional support or counseling in place of a qualified healthcare professional.
- Communicate emergency medical instructions without clinician review.

Patients should always have the opportunity to ask questions and receive explanations directly from a qualified healthcare professional.

Communicating About AI Use

When AI is used to assist with documentation, education, or administrative activities, employees should be prepared to answer patient questions honestly and transparently.

Patients may ask:

- What is Artificial Intelligence?
- How is AI used by the agency?
- Does AI make my healthcare decisions?
- Is my information protected?
- Who reviews AI-generated information?

Employees should explain that:

- AI is used only as a support tool for approved purposes.
- Licensed healthcare professionals make all clinical decisions.
- AI does not replace patient assessments or professional judgment.
- Patient information is protected according to HIPAA and agency policies.
- All AI-generated information is reviewed and verified before use.

Patient Education

During every appropriate visit, healthcare professionals should provide education tailored to the patient's needs, including:

- Disease process and management.
- Medication instructions.
- Safety and fall prevention.
- Infection prevention.
- Emergency preparedness.
- Use of medical equipment.
- Signs and symptoms requiring physician notification.
- Self-management strategies.
- Caregiver responsibilities when applicable.

Documentation should reflect the education provided, the patient's understanding, and any follow-up needs.

Communication with Caregivers

When appropriate and authorized, caregivers should be included in communication regarding:

- The patient's Plan of Care.
- Medication management.
- Safety precautions.
- Home exercise programs.
- Emergency planning.
- Follow-up appointments.
- Changes in the patient's condition.
- Care coordination with other healthcare providers.

Communication with caregivers must comply with HIPAA and patient authorization requirements.

Employee Responsibilities

Every workforce member is responsible for:

- Communicating respectfully and professionally.
- Protecting patient confidentiality.
- Verifying the accuracy of AI-assisted communications.
- Providing truthful and understandable information.
- Encouraging patients and caregivers to ask questions.
- Reporting communication concerns or misunderstandings that may affect patient safety.
- Following agency policies regarding AI use and patient communication.

Leadership Responsibilities

Agency leadership should:

- Establish policies governing AI-assisted patient communication.
- Ensure staff receive education on communication skills and responsible AI use.
- Monitor patient satisfaction and communication quality through the QAPI program.
- Review patient complaints related to communication.
- Promote a culture of transparency, respect, and patient-centered care.

Regulatory Considerations

Effective patient communication supports compliance with:

- CMS Home Health Conditions of Participation (42 CFR Part 484).
- Patient Rights requirements.
- HIPAA Privacy Rule.
- Agency policies regarding informed consent, confidentiality, and patient education.
- Quality Assessment and Performance Improvement (QAPI) requirements.

Key Takeaway

Clear, compassionate, and accurate communication is a fundamental responsibility of every healthcare professional. **Artificial Intelligence can assist with educational materials and administrative communication, but it cannot replace direct conversations, clinical judgment, or the therapeutic relationship between clinicians and patients. Patients have the right to receive understandable information, ask questions, participate in their care, and know that all AI-assisted communications are reviewed and verified by qualified healthcare professionals.**

- **AI-assisted voice documentation:** AI-assisted voice documentation uses speech recognition and Artificial Intelligence (AI) technologies to convert spoken words into clinical documentation. These tools may improve efficiency by allowing healthcare professionals to dictate visit notes, assessments, and other documentation rather than typing them manually. Although AI-assisted voice documentation can reduce administrative burden, **it is not a substitute for professional judgment or documentation responsibility.** Every entry generated through voice recognition or AI must be reviewed, corrected, and authenticated by the clinician before it becomes part of the patient's medical record.

What Is AI-Assisted Voice Documentation?

AI-assisted voice documentation combines:

- Speech-to-text technology.
- Natural Language Processing (NLP).
- AI-assisted summarization.
- Documentation templates.
- Clinical language recognition.

The technology converts spoken information into written documentation and may organize information into appropriate sections of the medical record.

Appropriate Uses

AI-assisted voice documentation may be used to:

- Dictate patient visit notes.
- Record assessment findings.
- Document patient education.
- Prepare draft progress notes.

- Improve documentation efficiency.
- Reduce manual typing.
- Assist with documentation organization.

The clinician must verify that the final documentation accurately reflects the care actually provided.

Limitations: AI-assisted voice documentation may:

- Misinterpret spoken words.
- Substitute incorrect medical terminology.
- Confuse medications, dosages, or diagnoses.
- Omit important assessment findings.
- Create grammatical or contextual errors.
- Produce AI hallucinations or unsupported statements.
- Misidentify speakers during conversations.
- Fail to recognize accents, background noise, or poor audio quality.

Because of these limitations, AI-generated documentation should never be accepted without careful review.

Risks: Improper use of AI-assisted voice documentation may result in:

- Inaccurate clinical documentation.
- Medication errors.
- Incorrect patient information.
- Documentation cloning.
- Copy-and-paste errors.
- Billing or coding inaccuracies.
- HIPAA violations if recordings are improperly stored or transmitted.
- Survey deficiencies.
- Potential False Claims Act exposure if inaccurate documentation supports billing.

Documentation Review Requirements

Before signing documentation, clinicians should verify:

- Patient identification.
- Assessment findings.
- Vital signs.
- Medications and dosages.
- Treatments provided.
- Patient response.
- Education provided.
- Physician notifications.
- Dates and times.
- Clinical terminology.
- Grammar and context.
- Completeness of the documentation.

Any inaccuracies should be corrected before the documentation becomes part of the medical record.

Privacy and HIPAA Considerations

When using AI-assisted voice documentation:

- Use only agency-approved voice documentation applications.
- Ensure the technology complies with HIPAA and agency privacy policies.
- Verify that a Business Associate Agreement (BAA) is in place when required.
- Protect recordings containing Protected Health Information (PHI).
- Avoid recording conversations on personal devices or unauthorized applications.
- Prevent unauthorized individuals from hearing or accessing dictated information.
- Secure mobile devices and workstations used for voice documentation.

AI Voice Recording Best Practices

Healthcare professionals should:

- Dictate in a private environment whenever possible.
- Speak clearly and accurately.

- Avoid abbreviations that may be misinterpreted.
- Review the completed documentation immediately after transcription.
- Correct recognition errors before signing.
- Ensure documentation reflects only observations made during the current visit.
- Individualize documentation for every patient encounter.
- Never rely solely on AI-generated summaries.

Employee Responsibilities

Every workforce member should:

- Use only agency-approved AI voice documentation systems.
- Verify the accuracy of every AI-generated note.
- Maintain patient confidentiality during dictation.
- Report software malfunctions or transcription errors.
- Follow agency documentation, privacy, and cybersecurity policies.
- Complete documentation promptly after each visit.

Leadership Responsibilities

Agency leadership should:

- Approve voice documentation technologies before implementation.
- Evaluate vendor privacy and security protections.
- Provide education and competency validation.
- Monitor documentation quality through the QAPI program.
- Audit AI-assisted documentation for accuracy and completeness.
- Investigate documentation errors associated with voice recognition technologies.
- Update policies as technology evolves.

Regulatory Considerations

AI-assisted voice documentation should support compliance with:

- CMS Home Health Conditions of Participation (42 CFR Part 484).
- HIPAA Privacy and Security Rules.
- Medicare documentation requirements.
- Agency documentation standards.
- Quality Assessment and Performance Improvement (QAPI) requirements.
- Fraud, Waste, and Abuse prevention policies.

Key Takeaway

AI-assisted voice documentation can improve efficiency and reduce administrative burden, but **it does not replace the clinician's responsibility for accurate, complete, and patient-specific documentation. Every AI-generated transcription must be carefully reviewed, corrected, and authenticated before it becomes part of the medical record. The clinician who signs the documentation remains fully accountable for its accuracy, regardless of how it was created.**

- **Remote work security:** Remote work allows employees to perform authorized agency duties from locations outside the traditional office, such as their home or another approved worksite. While remote work offers flexibility and may improve efficiency, it also increases the risk of unauthorized access to Protected Health Information (PHI), cybersecurity threats, and data breaches.

The agency is committed to protecting patient information, maintaining HIPAA compliance, and ensuring that all remote work is conducted securely. Employees who access agency systems remotely, including Artificial Intelligence (AI) applications, Electronic Health Records (EHRs), email, cloud-based services, or other technology resources, are responsible for safeguarding confidential information at all times.

Remote Work Risks

Working outside the agency's secure environment may increase the risk of:

- Unauthorized access to patient records.
- Loss or theft of laptops, tablets, or mobile devices.
- Use of unsecured Wi-Fi networks.
- Phishing attacks and social engineering.
- Malware or ransomware infections.

- Accidental disclosure of confidential information.
- Improper use of personal devices.
- Unauthorized use of AI applications containing PHI.
- Inadequate physical security of paper or electronic records.

Understanding these risks is essential to maintaining patient privacy and regulatory compliance.

Secure Remote Access

Employees should access agency systems remotely only through approved methods, such as:

- Agency-approved Virtual Private Network (VPN) connections.
- Secure cloud-based applications approved by the agency.
- Multi-Factor Authentication (MFA).
- Agency-issued devices whenever available.
- Encrypted internet connections.

Remote access should never bypass agency security controls.

Device Security

Employees should:

- Use agency-issued devices whenever possible.
- Install security updates promptly.
- Maintain antivirus and endpoint protection software.
- Enable automatic screen locking.
- Use strong passwords and Multi-Factor Authentication.
- Encrypt laptops, tablets, and mobile devices when supported.
- Prevent family members or unauthorized individuals from using agency devices.
- Report lost or stolen devices immediately.

Home Office Security

Employees working remotely should:

- Work in a private location whenever possible.
- Position computer screens to prevent unauthorized viewing.
- Lock the workstation whenever leaving the area.
- Store paper records securely.
- Prevent conversations containing PHI from being overheard.
- Shred confidential documents using approved methods before disposal.
- Secure mobile devices when traveling.

Network Security

Employees should:

- Use password-protected home Wi-Fi networks with strong encryption (WPA2 or WPA3).
- Change default router passwords.
- Avoid using public Wi-Fi when accessing agency information unless an approved VPN is used.
- Never disable security software.
- Disconnect from unsecured networks immediately.

Email and Communication Security

When working remotely, employees should:

- Use only agency-approved email accounts for business communications.
- Verify recipient addresses before sending confidential information.
- Avoid forwarding agency email to personal accounts.
- Use secure messaging platforms approved by the agency.
- Report suspicious emails or phishing attempts immediately.
- Never transmit PHI through unauthorized communication platforms.

AI and Remote Work

Employees using AI while working remotely should:

- Use only agency-approved AI applications.
- Never enter PHI into public or unauthorized AI platforms.
- Verify that AI systems comply with agency privacy and security requirements.

- Review all AI-generated information before incorporating it into documentation.
- Log out of AI applications when work is complete.
- Follow agency policies regarding AI use, documentation, and cybersecurity.

Physical Security of Information

Employees should:

- Keep paper records in secure locations.
- Never leave patient information unattended in vehicles or public places.
- Retrieve printed documents promptly from printers.
- Dispose of confidential documents using approved destruction methods.
- Prevent unauthorized individuals from viewing computer screens or printed records.

Incident Reporting

Employees must immediately report:

- Lost or stolen devices.
- Suspected data breaches.
- Unauthorized access to agency systems.
- Phishing emails or cybersecurity attacks.
- Accidental disclosure of PHI.
- Unauthorized use of AI applications.
- Any suspected compromise of agency information.

Prompt reporting allows the agency to investigate the incident, protect patient information, and comply with legal reporting requirements.

Employee Responsibilities

Every workforce member working remotely is responsible for:

- Following agency remote work policies.
- Protecting patient confidentiality.
- Using only approved devices and applications.
- Maintaining secure passwords and authentication methods.
- Verifying AI-generated information before use.
- Reporting cybersecurity concerns immediately.
- Completing required cybersecurity and AI education.

Leadership Responsibilities

Agency leadership should:

- Establish remote work security policies.
- Approve secure technologies and AI applications.
- Provide cybersecurity education and competency validation.
- Monitor compliance through audits and QAPI activities.
- Evaluate remote access risks.
- Investigate remote work security incidents.
- Update security controls as technology and threats evolve.

Regulatory Considerations

Remote work practices should support compliance with:

- HIPAA Privacy Rule.
- HIPAA Security Rule.
- CMS Home Health Conditions of Participation (42 CFR Part 484).
- Agency cybersecurity policies.
- AI governance policies.
- Quality Assessment and Performance Improvement (QAPI) requirements.

Key Takeaway

Remote work does not reduce an employee's responsibility to protect confidential information. **Every workforce member must maintain the same level of privacy, security, and professionalism when working remotely as when working in the office. Secure remote access, appropriate use of AI, strong cybersecurity practices, and**

immediate reporting of security incidents are essential to protecting patient information, maintaining regulatory compliance, and supporting safe, high-quality home health care.

- **Secure mobile device use**

Mobile devices, including smartphones, tablets, and laptops, are valuable tools that allow healthcare professionals to access electronic health records (EHRs), communicate with patients and providers, document care, and utilize approved Artificial Intelligence (AI) applications while providing services in patients' homes. However, these devices also present significant privacy and cybersecurity risks if they are not properly secured. The agency requires all workforce members to use mobile devices in a manner that protects Protected Health Information (PHI), complies with HIPAA, supports CMS Conditions of Participation, and follows agency cybersecurity and AI governance policies.

Mobile Devices Covered

This policy applies to:

- Agency-issued smartphones.
- Agency-issued tablets.
- Agency-issued laptops.
- Approved Bring Your Own Device (BYOD) devices, if permitted by agency policy.
- Mobile applications used for patient care, documentation, secure messaging, telehealth, scheduling, and approved AI functions.

Security Risks

Improper use of mobile devices may result in:

- Unauthorized access to patient records.
- Loss or theft of devices.
- Exposure of Protected Health Information (PHI).
- Malware or ransomware infections.
- Unauthorized use of AI applications.
- Data breaches.
- Identity theft.
- Regulatory violations.
- Financial penalties.
- Loss of patient trust.

Device Security Requirements

All mobile devices used for agency business should:

- Be protected with a strong password, PIN, or biometric authentication (such as fingerprint or facial recognition).
- Automatically lock after a short period of inactivity.
- Use Multi-Factor Authentication (MFA) whenever available.
- Have full-device encryption enabled whenever supported.
- Maintain current operating system and security updates.
- Use agency-approved antivirus or mobile security software when applicable.
- Allow remote lock and remote wipe capabilities for agency-issued devices.

Employees must never disable or bypass security features installed by the agency.

Approved Applications

Employees should use only agency-approved applications for:

- Electronic Health Records (EHR).
- Secure messaging.
- Email.
- Telehealth.
- Scheduling.
- Clinical documentation.
- Approved AI-assisted documentation or voice recognition.
- Patient education.

Applications downloaded from unknown or unauthorized sources should never be used for agency business.

AI Applications on Mobile Devices

When using AI on a mobile device, employees should:

- Use only agency-approved AI platforms.
- Never enter PHI into public AI applications.
- Verify all AI-generated information before using it.
- Log out of AI applications when work is complete.
- Ensure AI applications comply with HIPAA, agency privacy policies, and cybersecurity requirements.
- Report any suspected AI security or privacy concerns immediately.

Protecting Patient Information

Employees should:

- Access only the minimum necessary information needed to perform assigned duties.
- Avoid viewing patient records where screens may be visible to unauthorized individuals.
- Never leave mobile devices unattended in public areas.
- Lock devices whenever they are not in use.
- Avoid storing PHI on the device unless specifically authorized and encrypted.
- Delete temporary files containing confidential information according to agency policy.

Public Wi-Fi and Internet Use

Employees should:

- Use secure, password-protected networks whenever possible.
- Use the agency-approved Virtual Private Network (VPN) when accessing agency systems remotely.
- Avoid conducting agency business over unsecured public Wi-Fi unless protected by the approved VPN.
- Disable automatic connection to unknown wireless networks.
- Avoid using public charging stations that may expose devices to data theft ("juice jacking"). When charging away from home or the office, use a personal charger plugged directly into an electrical outlet or a USB data-blocking adapter.

Text Messaging and Communication

Employees should:

- Use only agency-approved secure messaging platforms.
- Never send PHI through personal text messages or unauthorized messaging applications.
- Verify recipient information before sending messages.
- Report messages sent to the wrong recipient immediately.
- Follow agency communication policies at all times.

Lost or Stolen Devices

If a mobile device used for agency business is lost or stolen, the employee should immediately:

- Notify their supervisor.
- Notify the Information Technology (IT) department or designated security officer.
- Report any potential exposure of PHI.
- Cooperate with remote lock or remote wipe procedures when applicable.
- Complete required incident reporting documentation.

Prompt reporting helps minimize the risk of unauthorized access and supports compliance with breach notification requirements.

Employee Responsibilities

Every workforce member is responsible for:

- Protecting agency-issued and approved personal devices.
- Using only authorized applications.
- Maintaining device security settings.
- Keeping software updated.
- Verifying AI-generated information before use.
- Protecting patient confidentiality.
- Reporting lost devices, suspected malware, phishing attempts, or other security incidents immediately.
- Completing required cybersecurity, HIPAA, and AI education.

Leadership Responsibilities

Agency leadership should:

- Establish policies governing mobile device security.
- Approve devices and applications used for agency business.
- Evaluate AI-enabled mobile technologies before implementation.
- Provide workforce education and competency validation.
- Monitor compliance through audits and the QAPI program.
- Investigate security incidents involving mobile devices.
- Update mobile security requirements as technology and cybersecurity threats evolve.

Regulatory Considerations

Secure mobile device use supports compliance with:

- HIPAA Privacy Rule.
- HIPAA Security Rule.
- CMS Home Health Conditions of Participation (42 CFR Part 484).
- HITECH Act requirements.
- Agency cybersecurity and AI governance policies.
- Quality Assessment and Performance Improvement (QAPI) requirements.

Key Takeaway

Mobile devices are essential tools for delivering home health services, but they must be used responsibly and securely. **Every workforce member is responsible for protecting mobile devices, safeguarding Protected Health Information, using only agency-approved AI and clinical applications, and maintaining compliance with HIPAA, CMS Conditions of Participation, and agency cybersecurity policies. Regardless of where care is provided, the employee who accesses or documents patient information remains accountable for its privacy, security, and accuracy.**

- **AI in interdisciplinary care:** Interdisciplinary care is a fundamental component of quality home health services. It involves collaboration among healthcare professionals from multiple disciplines to develop, implement, evaluate, and revise an individualized Plan of Care (POC) that addresses each patient's unique medical, functional, psychosocial, and educational needs.

Artificial Intelligence (AI) may assist the interdisciplinary team by improving communication, organizing clinical information, identifying trends, and supporting care coordination. However, **AI is a clinical support tool only and must never replace the professional judgment, responsibilities, or decision-making authority of licensed healthcare professionals.**

The Interdisciplinary Team

Depending on the patient's needs, the interdisciplinary team may include:

- Physician or Non-Physician Practitioner (NPP)
- Registered Nurse (RN)
- Licensed Practical Nurse (LPN), when permitted by state law and agency policy
- Physical Therapist (PT)
- Occupational Therapist (OT)
- Speech-Language Pathologist (SLP)
- Medical Social Worker (MSW)
- Home Health Aide (HHA)
- Registered Dietitian or Nutrition Professional, when ordered
- Administrator
- Director of Nursing (DON)
- Clinical Manager
- Other healthcare professionals involved in the patient's care

Each discipline contributes specialized knowledge and remains responsible for the services it provides.

Appropriate Uses of AI in Interdisciplinary Care

AI may assist the interdisciplinary team by:

- Summarizing clinical documentation for review.

- Organizing patient information from multiple disciplines.
- Identifying documentation inconsistencies.
- Highlighting changes or trends in patient condition.
- Assisting with care coordination.
- Supporting medication reconciliation reviews.
- Assisting with patient education materials.
- Preparing draft meeting agendas or interdisciplinary conference summaries.
- Identifying quality improvement opportunities through data analysis.

All AI-generated information must be reviewed and verified before it is used for patient care or documentation.

AI Does Not Replace Professional Judgment

AI must **never**:

- Determine a patient's diagnosis.
- Establish or revise the Plan of Care independently.
- Replace physician orders.
- Decide when services should begin, continue, or end.
- Perform patient assessments.
- Determine visit frequency.
- Replace interdisciplinary case conferences.
- Make discharge decisions.
- Replace clinical reasoning or professional accountability.

Clinical decisions must always be made by qualified healthcare professionals based on direct assessment, physician orders, evidence-based practice, and the patient's individual needs.

AI and Care Coordination

AI may improve care coordination by assisting with:

- Identifying overdue physician orders.
- Tracking care plan updates.
- Monitoring documentation completion.
- Identifying potential medication discrepancies.
- Organizing interdisciplinary communication.
- Highlighting unresolved clinical issues for review.
- Supporting QAPI performance monitoring.

AI recommendations should always be confirmed through clinical review before action is taken.

Communication Among Disciplines

Effective interdisciplinary communication should include:

- Timely sharing of significant patient changes.
- Collaboration regarding patient goals.
- Review of physician orders.
- Medication reconciliation.
- Coordination of patient education.
- Documentation of interventions and patient response.
- Planning for discharge and continuity of care.

AI may organize or summarize information but should never replace direct communication between team members.

Documentation Responsibilities

Each discipline remains responsible for:

- Completing timely and accurate documentation.
- Recording only services personally provided or supervised.
- Verifying any AI-assisted documentation.
- Documenting patient-specific findings.
- Communicating significant changes promptly.
- Maintaining compliance with agency documentation standards.

Documentation generated with AI assistance must accurately reflect the clinician's own assessment and interventions.

Human Oversight

Every member of the interdisciplinary team should:

- Independently review AI-generated information.
- Confirm recommendations using professional judgment.
- Verify information against the patient's assessment, physician orders, and Plan of Care.
- Correct inaccurate or incomplete AI-generated content.
- Report AI errors, hallucinations, or system concerns according to agency policy.

Employee Responsibilities

Every workforce member should:

- Collaborate respectfully with all members of the interdisciplinary team.
- Use AI only as an approved support tool.
- Protect patient confidentiality during interdisciplinary communication.
- Verify AI-generated summaries and recommendations before use.
- Participate in interdisciplinary conferences when appropriate.
- Report concerns regarding AI accuracy or documentation integrity.
- Follow agency policies regarding HIPAA, AI use, and documentation.

Leadership Responsibilities

Agency leadership should:

- Promote interdisciplinary collaboration.
- Establish policies governing AI-assisted care coordination.
- Provide education on AI capabilities and limitations.
- Monitor interdisciplinary documentation through the QAPI program.
- Evaluate AI performance for accuracy, fairness, and effectiveness.
- Investigate AI-related incidents affecting patient care.
- Ensure AI supports—not replaces—clinical teamwork and patient-centered care.

Regulatory Considerations

AI-assisted interdisciplinary care should support compliance with:

- CMS Home Health Conditions of Participation (42 CFR Part 484).
- HIPAA Privacy and Security Rules.
- Medicare documentation requirements.
- Patient Rights requirements.
- Quality Assessment and Performance Improvement (QAPI) requirements.
- Agency policies governing interdisciplinary care and AI use.

Key Takeaway

High-quality home health care depends on effective collaboration among all members of the interdisciplinary team. **Artificial Intelligence can improve communication, organization, and care coordination, but it cannot replace the expertise, professional judgment, or accountability of licensed healthcare professionals. Every discipline remains responsible for its own assessments, documentation, interventions, and clinical decisions, while working together to provide safe, individualized, and patient-centered care.**

- **Disaster recovery:** Disaster recovery is the process of restoring critical information systems, data, communications, and operational capabilities following a natural disaster, cyberattack, system failure, or other event that disrupts normal operations. In home health care, disaster recovery is essential to ensure the continuity of patient care, protect Protected Health Information (PHI), maintain regulatory compliance, and restore agency operations as quickly and safely as possible.

Artificial Intelligence (AI) technologies used by the agency must be included in disaster recovery planning to ensure they can be restored securely, continue to protect patient information, and support clinical operations without compromising patient safety or regulatory compliance.

Objectives of Disaster Recovery

The agency's disaster recovery program is designed to:

- Protect patient safety.

- Restore access to critical clinical information.
- Minimize operational downtime.
- Maintain continuity of patient care.
- Protect electronic Protected Health Information (ePHI).
- Restore communication systems.
- Recover critical business functions.
- Support compliance with HIPAA and CMS Conditions of Participation.
- Reduce the impact of cybersecurity incidents and technology failures.

Events That May Require Disaster Recovery

Disaster recovery procedures may be activated following events such as:

- Hurricanes, tornadoes, floods, or other natural disasters.
- Fires or structural damage.
- Extended power outages.
- Internet or telecommunications failures.
- Cybersecurity attacks, including ransomware or malware.
- Hardware or server failures.
- Electronic Health Record (EHR) outages.
- Cloud service interruptions.
- Loss of agency-issued mobile devices.
- AI system failures or data corruption.
- Other events that significantly disrupt agency operations.

Critical Systems

The agency should identify and prioritize systems that are essential to patient care and operations, including:

- Electronic Health Record (EHR) system.
- Clinical documentation systems.
- Scheduling and staffing software.
- Secure email and communication platforms.
- Telehealth services.
- Approved AI applications.
- Medication management systems.
- Payroll and human resources systems.
- Financial and billing systems.
- Backup and data recovery systems.

Data Backup and Recovery

To protect agency information, the agency should:

- Perform routine backups of critical electronic data.
- Store backups in secure, encrypted locations.
- Maintain redundant backup systems whenever practical.
- Test backup restoration procedures periodically.
- Verify the integrity of recovered data before returning systems to production.
- Protect backup media from unauthorized access or damage.

AI System Recovery

If AI systems become unavailable or compromised:

- Patient care should continue using established manual or alternative procedures.
- Clinicians should not delay necessary patient care while waiting for AI services to be restored.
- AI-generated documentation that has not been reviewed and authenticated should not be used.
- Restored AI systems should be tested to confirm accuracy, security, and functionality before returning to service.
- AI vendors should be notified when required under contractual agreements.

Cybersecurity Incident Recovery

Following a cybersecurity incident, the agency should:

- Isolate affected systems when appropriate.

- Notify Information Technology (IT) personnel or contracted technology support.
- Assess the scope and impact of the incident.
- Restore systems from verified backups when appropriate.
- Change passwords and authentication credentials as necessary.
- Verify that malware or unauthorized access has been eliminated.
- Evaluate whether breach notification requirements apply.
- Document all recovery activities.

Continuity of Patient Care

During technology disruptions, employees should:

- Follow the agency's Emergency Preparedness and Business Continuity Plans.
- Use approved downtime procedures for documentation.
- Continue providing medically necessary patient care.
- Communicate with physicians, patients, caregivers, and other providers regarding any service interruptions.
- Restore documentation to the Electronic Health Record as soon as systems become available.
- Verify the accuracy and completeness of all delayed documentation.

Testing and Training

The agency should:

- Test disaster recovery procedures on a regular basis.
- Include AI systems in disaster recovery exercises when applicable.
- Conduct periodic cybersecurity incident simulations.
- Educate workforce members on disaster recovery responsibilities.
- Review lessons learned after actual events or exercises.
- Update disaster recovery procedures based on identified improvements.

Employee Responsibilities

Every workforce member should:

- Know how to report technology failures immediately.
- Follow agency downtime and disaster recovery procedures.
- Protect patient confidentiality during system outages.
- Use only approved backup documentation methods.
- Verify documentation entered after system restoration.
- Report suspected cybersecurity incidents promptly.
- Participate in required disaster recovery and emergency preparedness training.

Leadership Responsibilities

Agency leadership should:

- Maintain a written Disaster Recovery Plan.
- Coordinate disaster recovery activities with the Emergency Preparedness Program.
- Ensure secure backups of critical data.
- Evaluate AI vendors' disaster recovery capabilities before implementation.
- Conduct periodic testing of recovery procedures.
- Monitor recovery effectiveness through the QAPI program.
- Review and revise disaster recovery plans after significant events or technology changes.

Regulatory Considerations

Disaster recovery planning supports compliance with:

- HIPAA Security Rule (Contingency Plan requirements).
- HIPAA Privacy Rule.
- CMS Home Health Conditions of Participation (42 CFR Part 484).
- Emergency Preparedness Requirements (42 CFR Part 484.102).
- Agency cybersecurity policies.
- AI governance policies.
- Quality Assessment and Performance Improvement (QAPI) requirements.

Key Takeaway

Disaster recovery ensures that the agency can restore critical technology, protect patient information, and continue delivering safe, high-quality home health services following a disruption. **Artificial Intelligence may enhance agency operations, but patient care must never depend solely on AI availability. Every workforce member should be prepared to follow downtime procedures, protect patient information, and support the secure restoration of agency systems while maintaining compliance with HIPAA, CMS Conditions of Participation, and the agency's Emergency Preparedness and Disaster Recovery Plans.**

- **Business continuity:** Business Continuity is the agency's ability to maintain or rapidly resume essential operations during and after a disruption while continuing to provide safe, effective, and compliant patient care. Business continuity planning ensures that critical clinical, administrative, financial, and technological functions continue despite emergencies such as natural disasters, cybersecurity incidents, power failures, pandemics, or other unexpected events. Artificial Intelligence (AI) technologies may support agency operations; however, **business continuity planning must ensure that patient care can continue safely even if AI systems or other technology become unavailable.**

Objectives of Business Continuity

The agency's Business Continuity Program is designed to:

- Maintain uninterrupted patient care whenever possible.
- Protect the health and safety of patients, caregivers, employees, and visitors.
- Preserve access to critical patient information.
- Maintain compliance with federal and state regulations.
- Minimize operational disruptions.
- Protect agency assets and information systems.
- Restore normal operations efficiently.
- Ensure continuity of communication with patients, physicians, referral sources, vendors, and regulatory agencies.
- Support financial and operational stability during emergencies.

Events That May Disrupt Operations

Business continuity procedures may be activated during events such as:

- Hurricanes, tornadoes, floods, or severe weather.
- Fires or structural damage.
- Public health emergencies or pandemics.
- Cybersecurity attacks, including ransomware.
- Extended power or internet outages.
- Electronic Health Record (EHR) system failures.
- AI system failures.
- Telecommunications disruptions.
- Supply chain interruptions.
- Workforce shortages.
- Civil emergencies or community disasters.
- Other incidents affecting agency operations.

Essential Business Functions

The agency should identify and prioritize critical functions necessary to continue operations, including:

Clinical Operations

- Patient assessments.
- Skilled nursing and therapy visits.
- Home Health Aide services.
- Physician communication.
- Medication management.
- Emergency patient triage.
- Continuity of the individualized Plan of Care.

Administrative Operations

- Scheduling.
- Patient intake and admissions.

- Human resources.
- Payroll.
- Billing and reimbursement.
- Quality Assessment and Performance Improvement (QAPI).
- Regulatory reporting.
- Medical records management.

Technology Services

- Electronic Health Record (EHR).
- Secure communications.
- Approved AI applications.
- Telehealth platforms.
- Data backup systems.
- Cybersecurity monitoring.

AI and Business Continuity

Artificial Intelligence may support:

- Documentation assistance.
- Care coordination.
- Scheduling support.
- Clinical information organization.
- Quality improvement analysis.
- Administrative workflow.

However:

- AI must never become the sole method of providing patient care.
- Clinicians must be prepared to continue documentation manually when necessary.
- Clinical decisions must not be delayed because AI systems are unavailable.
- Patient care always takes priority over technology.

Continuity of Patient Care

During disruptions, employees should:

- Prioritize patients based on clinical needs.
- Contact high-risk patients promptly.
- Coordinate care with physicians and other providers.
- Follow the agency's Emergency Preparedness Plan.
- Implement approved downtime documentation procedures.
- Maintain communication with patients and caregivers.
- Resume normal documentation once systems are restored.
- Ensure all delayed documentation is accurate and complete.

Communication Plan

The agency should maintain reliable methods to communicate with:

- Patients.
- Caregivers.
- Physicians.
- Hospitals.
- Referral sources.
- Employees.
- Vendors.
- Regulatory agencies.
- Emergency management officials.

Alternative communication methods should be available if primary systems become unavailable.

Workforce Continuity

To maintain operations, the agency should:

- Identify essential personnel.
- Cross-train employees for critical functions when appropriate.

- Maintain updated emergency contact information.
- Establish succession plans for key leadership positions.
- Develop staffing contingency plans.
- Provide employees with emergency preparedness education.

Supply and Resource Management

The agency should:

- Maintain access to essential medical supplies.
- Identify backup vendors when possible.
- Monitor inventory during emergencies.
- Coordinate with community resources.
- Ensure critical equipment remains available for patient care.

Cybersecurity and Information Protection

Business continuity planning should include:

- Secure backup systems.
- Data recovery procedures.
- Cybersecurity incident response.
- Protection of Protected Health Information (PHI).
- AI system recovery procedures.
- Secure remote access capabilities.
- Ongoing monitoring of system integrity after restoration.

Testing and Exercises

The agency should periodically:

- Conduct business continuity exercises.
- Test downtime procedures.
- Evaluate communication systems.
- Test recovery of Electronic Health Records and critical applications.
- Include AI system outages in continuity drills.
- Review lessons learned and update procedures.

Employee Responsibilities

Every workforce member should:

- Understand the agency's Business Continuity Plan.
- Know their assigned responsibilities during emergencies.
- Protect patient confidentiality during operational disruptions.
- Follow downtime documentation procedures.
- Continue providing safe, patient-centered care.
- Report operational or cybersecurity issues promptly.
- Participate in required emergency preparedness and business continuity training.

Leadership Responsibilities

Agency leadership should:

- Maintain and periodically review the Business Continuity Plan.
- Coordinate business continuity with the Emergency Preparedness Program.
- Ensure critical operations can continue during disruptions.
- Evaluate the resilience of AI vendors and technology partners.
- Monitor continuity performance through the QAPI program.
- Conduct after-action reviews following significant events.
- Update policies based on regulatory changes, technology advancements, and lessons learned.

Regulatory Considerations

Business continuity planning supports compliance with:

- CMS Home Health Conditions of Participation (42 CFR Part 484).
- Emergency Preparedness Requirements (42 CFR Part 484.102).
- HIPAA Privacy and Security Rules.
- HITECH Act requirements.

- Agency cybersecurity and AI governance policies.
- Quality Assessment and Performance Improvement (QAPI) requirements.

Key Takeaway

Business continuity ensures that the agency can continue delivering safe, effective, and compliant home health services during and after operational disruptions. **Artificial Intelligence is a valuable support tool, but patient care, clinical judgment, and regulatory responsibilities must never depend solely on technology. Every workforce member plays a critical role in maintaining continuity of operations, protecting patient information, communicating effectively, and ensuring uninterrupted care during emergencies.**

- **AI performance monitoring:** Artificial Intelligence (AI) performance monitoring is the ongoing process of evaluating AI systems to ensure they function accurately, securely, reliably, ethically, and in compliance with applicable laws, regulations, and agency policies. Continuous monitoring helps identify errors, system degradation, bias, cybersecurity risks, and opportunities for improvement before they affect patient care or agency operations. The agency is committed to regularly monitoring all approved AI technologies to ensure they support safe, high-quality, patient-centered care while maintaining compliance with the **CMS Home Health Conditions of Participation (CoPs), HIPAA, Medicare documentation requirements, and the agency's Quality Assessment and Performance Improvement (QAPI) Program.**

Objectives of AI Performance Monitoring

The agency's AI performance monitoring program is designed to:

- Verify the accuracy and reliability of AI-generated information.
- Detect AI hallucinations, errors, and inaccurate recommendations.
- Monitor documentation quality and completeness.
- Evaluate AI system performance over time.
- Identify cybersecurity and privacy concerns.
- Detect algorithmic bias or unfair outcomes.
- Ensure continued compliance with agency policies.
- Support continuous quality improvement.
- Reduce patient safety risks.
- Protect the integrity of clinical documentation.

What Should Be Monitored?

The agency should routinely monitor AI systems for:

Accuracy

- Correct clinical terminology.
- Accurate documentation summaries.
- Appropriate recommendations.
- Consistency with physician orders.
- Compliance with evidence-based practice.

Documentation Quality

- Individualized patient documentation.
- Completeness of clinical notes.
- Proper medication documentation.
- Accurate care coordination.
- Appropriate patient education documentation.
- Documentation integrity and authenticity.

AI Hallucinations

Monitor for:

- Fabricated patient information.
- Incorrect medications or dosages.
- False diagnoses.
- Unsupported clinical recommendations.
- Incorrect regulatory references.
- Inaccurate citations or references.

Bias and Fairness

Evaluate AI outputs for:

- Consistent recommendations across patient populations.
- Potential discriminatory patterns.
- Cultural and linguistic appropriateness.
- Fair treatment of all patients.
- Compliance with nondiscrimination principles.

Privacy and Security

Monitor for:

- Unauthorized disclosure of Protected Health Information (PHI).
- Improper AI data use.
- Unauthorized system access.
- Cybersecurity vulnerabilities.
- Compliance with HIPAA requirements.

Operational Performance

Evaluate:

- System availability.
- Response times.
- Downtime frequency.
- Software updates.
- Vendor performance.
- Integration with Electronic Health Records (EHR).

Performance Indicators (KPIs)

Examples of Key Performance Indicators (KPIs) include:

- AI documentation accuracy rate.
- Percentage of AI-generated notes requiring correction.
- Number of identified AI hallucinations.
- Medication documentation error rate.
- AI-related incident reports.
- Documentation completion time.
- User satisfaction.
- AI system uptime.
- Security incidents involving AI.
- Number of privacy violations.
- AI competency completion rates.
- AI training compliance rates.

Monitoring Methods

The agency may evaluate AI performance through:

- Clinical documentation audits.
- Peer review.
- QAPI chart reviews.
- Random quality assurance audits.
- Incident reporting.
- Employee feedback.
- Vendor performance reports.
- Cybersecurity monitoring.
- AI system testing after updates.
- Patient complaints or concerns involving AI-assisted services.

Human Oversight

Every AI-generated output should be reviewed by qualified personnel before it is relied upon for patient care or official documentation.

Healthcare professionals should:

- Verify AI-generated information.

- Correct inaccurate or incomplete outputs.
- Reject AI recommendations that conflict with clinical judgment or physician orders.
- Report recurring AI issues to leadership.

Human oversight remains mandatory regardless of AI performance.

Incident Investigation

If monitoring identifies significant AI issues, the agency should:

- Investigate the event promptly.
- Determine the root cause.
- Assess patient safety impact.
- Correct inaccurate documentation when appropriate.
- Notify the AI vendor if necessary.
- Implement corrective actions.
- Monitor for recurrence through QAPI activities.

Employee Responsibilities

Every workforce member should:

- Use only agency-approved AI systems.
- Review all AI-generated documentation before finalizing it.
- Report suspected AI errors, hallucinations, bias, or security concerns.
- Participate in AI competency validation and ongoing education.
- Follow agency documentation, cybersecurity, and AI governance policies.
- Cooperate with quality audits and performance reviews.

Leadership Responsibilities

Agency leadership should:

- Establish an AI performance monitoring program.
- Define measurable AI performance standards.
- Monitor AI performance through the QAPI Program.
- Review audit findings and performance trends.
- Evaluate vendor performance regularly.
- Investigate AI-related incidents.
- Implement corrective and preventive actions.
- Update AI policies as technology evolves.
- Report significant findings to the Governing Body and Quality Committee when appropriate.

Integration with QAPI

AI performance monitoring should be incorporated into the agency's **Quality Assessment and Performance Improvement (QAPI) Program** by:

- Including AI metrics on quality dashboards.
- Reviewing AI performance during Quality Committee meetings.
- Trending AI-related incidents over time.
- Initiating Performance Improvement Projects (PIPs) when recurring issues are identified.
- Evaluating the effectiveness of corrective actions.
- Using monitoring results to improve staff education and AI governance.

Regulatory Considerations

AI performance monitoring supports compliance with:

- CMS Home Health Conditions of Participation (42 CFR Part 484).
- Quality Assessment and Performance Improvement (QAPI) requirements.
- HIPAA Privacy and Security Rules.
- Medicare documentation requirements.
- Agency AI governance policies.
- Cybersecurity and risk management policies.
- Fraud, Waste, and Abuse prevention requirements.

Key Takeaway

Continuous AI performance monitoring is essential to ensuring that AI technologies remain safe, accurate, secure, and effective. **Artificial Intelligence should continuously earn the trust placed in it through regular evaluation, human oversight, and quality improvement. Every workforce member shares responsibility for identifying AI errors, protecting patient information, and ensuring that AI enhances—rather than compromises—patient care, documentation integrity, and regulatory compliance.**

- **Competency validation:** Competency validation is the formal process used to verify that workforce members possess the knowledge, skills, and abilities necessary to safely, ethically, and effectively use Artificial Intelligence (AI) technologies in the home health setting. Competency validation ensures that employees understand the capabilities and limitations of AI, comply with agency policies, protect patient privacy, and maintain responsibility for all clinical and administrative decisions.

Consistent with the **CMS Home Health Conditions of Participation (CoPs)** and the agency's commitment to quality care, **all workforce members who use AI must successfully complete competency validation before being granted access to AI technologies and at least annually thereafter.**

Objectives of Competency Validation

The agency's competency validation program is designed to ensure employees can:

- Understand basic AI concepts and terminology.
- Recognize the capabilities and limitations of AI.
- Demonstrate appropriate human oversight of AI-generated information.
- Verify the accuracy of AI-assisted documentation.
- Recognize AI hallucinations, bias, and inaccurate outputs.
- Protect Protected Health Information (PHI).
- Comply with HIPAA, CMS Conditions of Participation, Medicare requirements, and agency policies.
- Use only agency-approved AI technologies.
- Report AI-related concerns, incidents, or security issues appropriately.
- Apply ethical principles when using AI in patient care and administrative activities.

Employees Required to Complete Competency Validation

Competency validation applies to all workforce members who use AI, including but not limited to:

- Administrators.
- Director of Nursing (DON).
- Clinical Managers.
- Registered Nurses (RNs).
- Licensed Practical Nurses (LPNs), when applicable.
- Physical Therapists (PTs).
- Occupational Therapists (OTs).
- Speech-Language Pathologists (SLPs).
- Medical Social Workers (MSWs).
- Home Health Aides (HHAs), if authorized to use AI-supported technologies.
- Quality Assurance personnel.
- Scheduling and intake staff.
- Billing personnel.
- Human Resources staff.
- Information Technology personnel.
- Contract staff with authorized access to agency AI systems.

Timing of Competency Validation

Competency validation should occur:

- Before initial access to AI technologies.
- During new employee orientation when AI use is part of assigned responsibilities.
- At least annually thereafter.
- Whenever significant AI system changes are implemented.
- Following major policy revisions.
- Following identification of performance deficiencies.
- After AI-related incidents when retraining is indicated.

Competency Evaluation Methods

Competency may be validated through one or more of the following:

- Written examinations.
- Knowledge assessments.
- Case studies.
- Scenario-based exercises.
- Demonstration of AI-assisted documentation.
- Direct observation.
- Skills checklists.
- Documentation audits.
- Mock patient scenarios.
- Peer review.
- Supervisor evaluation.
- Question-and-answer discussions.
- Return demonstrations for AI-enabled documentation workflows.

Core Competencies

Employees should demonstrate competency in the following areas:

AI Fundamentals

- Basic AI concepts.
- Machine Learning overview.
- Generative AI overview.
- AI terminology.
- Capabilities and limitations.

Agency AI Policy

- Approved AI uses.
- Prohibited AI uses.
- Human oversight requirements.
- Documentation standards.
- Employee responsibilities.

Documentation

- Verification of AI-generated documentation.
- Prevention of documentation cloning.
- Recognition of AI hallucinations.
- Individualized patient documentation.
- Medicare documentation requirements.

Privacy and Security

- HIPAA compliance.
- Protection of PHI.
- Cybersecurity awareness.
- Secure AI use.
- Secure mobile device use.
- Remote work security.

Clinical Decision-Making

- Human oversight.
- Professional judgment.
- Patient-centered care.
- Clinical accountability.
- Physician communication.

Compliance and Ethics

- CMS Conditions of Participation.
- Fraud, Waste, and Abuse prevention.
- False Claims Act awareness.

- Bias mitigation.
- Ethical AI use.
- Patient rights.

Performance Expectations

Employees should be able to:

- Explain how AI is used within the agency.
- Identify situations where AI should not be used.
- Detect inaccurate AI-generated information.
- Correct AI-generated documentation before finalization.
- Protect patient confidentiality.
- Report AI incidents appropriately.
- Demonstrate safe and compliant AI use during routine job responsibilities.

Remediation

Employees who do not successfully demonstrate competency should:

- Receive additional education.
- Participate in individualized coaching.
- Repeat competency validation.
- Be supervised until competency is demonstrated.
- Have AI access restricted or suspended when necessary to protect patient safety and agency compliance.

Documentation of Competency

Competency records should include: Employee name and position. Date of validation. Topics evaluated. Evaluation method. Competency results. Name and credentials of the evaluator. Corrective education provided, if applicable. Employee and evaluator signatures, when required by agency policy. Competency records should be maintained in the employee's personnel file in accordance with agency record retention policies.

Leadership Responsibilities

Agency leadership should:

- Develop and maintain AI competency standards.
- Ensure competency validation is completed before AI access is granted.
- Provide annual education and refresher training.
- Monitor competency completion rates.
- Review competency results through the QAPI Program.
- Identify trends requiring additional education.
- Update competency tools as AI technology evolves.

Integration with QAPI

Competency validation should be incorporated into the **Quality Assessment and Performance Improvement (QAPI) Program** by:

- Monitoring annual competency completion rates.
- Reviewing documentation audit results.
- Tracking AI-related incidents associated with user performance.
- Evaluating the effectiveness of education programs.
- Implementing Performance Improvement Projects (PIPs) when recurring competency deficiencies are identified.

Regulatory Considerations

Competency validation supports compliance with:

- CMS Home Health Conditions of Participation (42 CFR Part 484).
- HIPAA Privacy and Security Rules.
- Medicare documentation requirements.
- Agency AI governance policies.
- Quality Assessment and Performance Improvement (QAPI) requirements.
- Fraud, Waste, and Abuse prevention requirements.

Key Takeaway: Competency validation ensures that every workforce member who uses Artificial Intelligence possesses the knowledge and skills necessary to do so safely, ethically, and in compliance with regulatory requirements. **Successful completion of AI education alone is not sufficient - employees must demonstrate their ability to apply that knowledge in daily practice. Regardless of AI assistance, each workforce member remains personally responsible for protecting patient information, exercising professional judgment, verifying AI-generated content, and maintaining the accuracy and integrity of the medical record.**

Knowledge Checks

1. Can AI replace licensed clinicians?
 - ☐ Yes
 - ☒ No
 2. Who is responsible for documentation accuracy?
 - ☐ AI
 - ☒ The clinician
 3. Should PHI be entered into unauthorized AI systems?
 - ☐ Yes
 - ☒ No
 4. Can AI assist with education and administrative work?
 - ☒ Yes
 - ☐ No
 5. Should AI-generated content always be reviewed?
 - ☒ Yes
 - ☐ No
-

Final Examination

Instructions: Select the best answer. Verbally practice (INSTRUCTOR-STAFF)

1. AI is primarily:
 - A. A replacement for nurses
 - **B. A tool that assists staff**
 - C. A physician
 - D. A surveyor
 2. Who remains responsible for clinical decisions?
 - A. AI
 - **B. Licensed healthcare professionals**
 - C. Software vendors
 - D. Patients
 3. AI-generated documentation must:
 - A. Be signed immediately
 - **B. Be reviewed and verified**
 - C. Never be edited
 - D. Replace assessments
 4. Which is an example of fraud?
 - A. Reviewing AI output
 - **B. Creating documentation for services not provided**
 - C. Using AI for education
 - D. Formatting a policy
 5. AI hallucinations are:
 - A. Hardware failures
 - **B. Incorrect or fabricated AI information**
 - C. Password problems
 - D. Survey deficiencies
-

Forms & Competencies

All professional forms, including:

- AI Risk Assessment
- Vendor Evaluation
- Security Assessment
- Implementation Readiness
- User Authorization
- Documentation Review
- Clinical Validation
- Incident Report
- Privacy Breach Report
- Quarterly Audit Tool
- QAPI Dashboard
- Corrective Action Plan
- Annual Policy Review
- Vendor Performance Evaluation
- Annual Competency

SAMPLE

Artificial Intelligence (AI) Risk Assessment Tool

Complete prior to implementation of any AI application or major software update.

AI Application Name:		Vendor:	
Version:		Assessment Date:	
Department(s):		Completed By:	

SECTION A – CLINICAL RISK ASSESSMENT

Assessment Item	Low	Moderate	High	Comments
May affect patient safety	☐	☐	☐	
May affect clinical decision-making	☐	☐	☐	
May affect documentation accuracy	☐	☐	☐	
May affect medication documentation	☐	☐	☐	
May affect OASIS documentation	☐	☐	☐	
May affect physician orders	☐	☐	☐	
May affect care planning	☐	☐	☐	
May affect patient education	☐	☐	☐	
May affect continuity of care	☐	☐	☐	

SECTION B – PRIVACY & HIPAA RISK

Assessment Item	Yes	No	Comments
Uses Protected Health Information (PHI)	☐	☐	
HIPAA compliance verified	☐	☐	
Business Associate Agreement completed (if applicable)	☐	☐	
Minimum Necessary Standard supported	☐	☐	
Data encrypted in transit	☐	☐	
Data encrypted at rest	☐	☐	
Vendor privacy review completed	☐	☐	
Access controls verified	☐	☐	
Audit logs available	☐	☐	
Role-based access available	☐	☐	

Comments: _____

Artificial Intelligence (AI) Risk Assessment Tool (cont'd)

SECTION C – CYBERSECURITY REVIEW

Assessment Item	Yes	No	Comments
Security Risk Assessment completed	☐	☐	
Vulnerability assessment completed	☐	☐	
Penetration testing completed (if applicable)	☐	☐	
Multi-factor authentication available	☐	☐	
Backup procedures verified	☐	☐	
Disaster recovery reviewed	☐	☐	
Business continuity reviewed	☐	☐	
Incident response procedures reviewed	☐	☐	
Vendor security certifications reviewed	☐	☐	

SECTION D – CLINICAL VALIDATION

Assessment Item	Yes	No	Comments
Clinical testing completed	☐	☐	
Documentation accuracy acceptable	☐	☐	
Voice transcription validated	☐	☐	
Medication documentation verified	☐	☐	
OASIS support validated	☐	☐	
ICD-10 suggestions reviewed	☐	☐	
Human review process verified	☐	☐	
Workflow testing completed	☐	☐	

SECTION E – VENDOR REVIEW

Assessment Item	Yes	No	Comments
Vendor approved	☐	☐	
HIPAA compliant	☐	☐	
BAA executed (if applicable)	☐	☐	
Service Level Agreement reviewed	☐	☐	
Technical support available	☐	☐	
Downtime procedures reviewed	☐	☐	
Update process verified	☐	☐	
Security patch process reviewed	☐	☐	

Comments: _____

Artificial Intelligence (AI) Risk Assessment Tool (cont'd)

SECTION F – OPERATIONAL REVIEW

Assessment Item	Yes	No	Comments
Staff training completed	☐	☐	
Policies updated	☐	☐	
User Acceptance Testing completed	☐	☐	
Pilot testing completed	☐	☐	
Workflow approved	☐	☐	
User access assigned	☐	☐	
Documentation standards reviewed	☐	☐	

Overall Implementation Risk: ☐ Low ☐ Moderate ☐ High

Identified Risks:

Mitigation Plan:

Final Recommendation: ☐ Approved ☐ Approved with Corrective Actions ☐ Pilot Required ☐ Not Approved

Approvals

Clinical Manager _____ Date _____

Director of Nursing _____ Date _____

Privacy/Security Officer _____ Date _____

Administrator _____ Date _____

AI Oversight Committee Chair _____ Date _____

AI VENDOR EVALUATION CHECKLIST

Complete prior to approving any Artificial Intelligence (AI) vendor for Agency use.

Vendor Name:		Product:	
Contact:		Version:	
Evaluation Date:		Evaluator:	

HIPAA & REGULATORY COMPLIANCE

Requirement	Yes	No	N/A	Comments
HIPAA compliance verified	☐	☐	☐	
Business Associate Agreement (BAA) available (if applicable)	☐	☐	☐	
HITECH compliance	☐	☐	☐	
CMS requirements supported	☐	☐	☐	
Florida regulations considered	☐	☐	☐	

SECURITY

Requirement	Yes	No	N/A	Comments
Encryption in transit	☐	☐	☐	
Encryption at rest	☐	☐	☐	
Role-based access	☐	☐	☐	
Multi-factor authentication available	☐	☐	☐	
Audit logs available	☐	☐	☐	
Incident response process documented	☐	☐	☐	
Disaster recovery plan available	☐	☐	☐	

VENDOR CAPABILITIES

Requirement	Yes	No	N/A	Comments
Technical support available	☐	☐	☐	
Training resources provided	☐	☐	☐	
Software updates and patch management	☐	☐	☐	
Downtime procedures documented	☐	☐	☐	
Service Level Agreement reviewed	☐	☐	☐	
Healthcare references available	☐	☐	☐	

DATA MANAGEMENT AI VENDOR EVALUATION CHECKLIST

Requirement	Yes	No	N/A	Comments
Data ownership defined	☐	☐	☐	
Data retention policy reviewed	☐	☐	☐	
Secure data deletion available	☐	☐	☐	
Backup procedures verified	☐	☐	☐	
Export capability available	☐	☐	☐	

OVERALL ASSESSMENT

Requirement	Yes	No	N/A	Comments
Clinical needs met	☐	☐	☐	
Operational needs met	☐	☐	☐	
Privacy requirements met	☐	☐	☐	
Security requirements met	☐	☐	☐	
Approved for implementation	☐	☐	☐	

Overall Recommendation

- ☐ Approved
 ☐ Approved with Conditions
 ☐ Additional Review Required
☐ Not Approved

Comments:

Approvals

Clinical Manager _____ Date _____
 Privacy/Security Officer _____ Date _____
 Administrator _____ Date _____
 AI Oversight Committee(BD) _____ Date _____

AI SECURITY ASSESSMENT CHECKLIST

Complete before implementing or renewing any Artificial Intelligence (AI) application that creates, receives, maintains, processes, stores, or transmits Protected Health Information (PHI).

AI Application:		Vendor:	
Version:		Assessment Date:	
Evaluator:		Department:	

ACCESS CONTROL

Assessment Item	Yes	No	N/A	Comments
Unique user IDs	☐	☐	☒	
Role-based access	☐	☐	☐	
Least privilege implemented	☐	☐	☐	
Account lockout	☐	☐	☐	
Automatic session timeout	☐	☐	☐	
Multi-factor authentication	☐	☐	☐	

DATA PROTECTION

Assessment Item	Yes	No	N/A	Comments
Encryption in transit	☐	☐	☐	
Encryption at rest	☐	☐	☐	
Secure backups	☐	☐	☐	
Secure data deletion	☐	☐	☐	
Data retention policy reviewed	☐	☐	☐	

SYSTEM SECURITY

Assessment Item	Yes	No	N/A	Comments
Security risk assessment completed	☐	☐	☐	
Vulnerability assessment completed	☐	☐	☐	
Penetration testing (if applicable)	☐	☐	☐	
Anti-malware protection	☐	☐	☐	
Patch/update process documented	☐	☐	☐	
System monitoring enabled	☐	☐	☐	

HIPAA & PRIVACY AI SECURITY ASSESSMENT CHECKLIST

Assessment Item	Yes	No	N/A	Comments
HIPAA compliance verified	☐	☐	☐	
Business Associate Agreement (if applicable)	☐	☐	☐	
Audit logging enabled	☐	☐	☐	
Minimum Necessary Standard supported	☐	☐	☐	
Privacy notice reviewed	☐	☐	☐	

BUSINESS CONTINUITY

Assessment Item	Yes	No	N/A	Comments
Disaster recovery plan	☐	☐	☐	
Business continuity plan	☐	☐	☐	
Downtime procedures	☐	☐	☐	
Incident response plan	☐	☐	☐	
Vendor emergency contacts available	☐	☐	☐	

Overall Security Assessment

☐ Acceptable Risk ☐ Acceptable with Corrective Actions ☐ High Risk-Do Not Implement

Corrective Actions / Comments: _____

Approvals

Information Security Officer _____ Date _____

Privacy Officer _____ Date _____

Administrator _____ Date _____

AI Oversight Committee (BD) _____ Date _____

AI IMPLEMENTATION READINESS CHECKLIST

Complete this checklist before implementing any Artificial Intelligence (AI) solution within the Home Health Agency.

AI Application:		Vendor:	
Department:		Go-Live Date:	
Project Lead:		Assessment Date:	

GOVERNANCE & APPROVALS

Readiness Item	Complete	Incomplete	N/A	Comments
AI Risk Assessment completed	☐	☐	☐	
Vendor Evaluation completed	☐	☐	☐	
Security Assessment completed	☐	☐	☐	
Governing Body approval obtained	☐	☐	☐	
AI Oversight Committee approval	☐	☐	☐	

REGULATORY COMPLIANCE

Readiness Item	Complete	Incomplete	N/A	Comments
HIPAA compliance verified	☐	☐	☐	
Business Associate Agreement executed (if applicable)	☐	☐	☐	
CMS Conditions of Participation reviewed	☐	☐	☐	
Agency policies updated	☐	☐	☐	

TECHNICAL READINESS

Readiness Item	Complete	Incomplete	N/A	Comments
System configuration completed	☐	☐	☐	
User accounts created	☐	☐	☐	
Role-based access verified	☐	☐	☐	
Encryption verified	☐	☐	☐	
Backup procedures tested	☐	☐	☐	
Downtime procedures established	☐	☐	☐	

CLINICAL READINESS AI IMPLEMENTATION READINESS CHECKLIST

Readiness Item	Complete	Incomplete	N/A	Comments
Clinical validation completed	☐	☐	☐	
Workflow testing completed	☐	☐	☐	
Pilot testing completed (if applicable)	☐	☐	☐	
Documentation standards reviewed	☐	☐	☐	
Human oversight process established	☐	☐	☐	

WORKFORCE PREPAREDNESS

Readiness Item	Complete	Incomplete	N/A	Comments
Staff training completed	☐	☐	☐	
Annual competency requirements established	☐	☐	☐	
Patient notification process ready	☐	☐	☐	
Support resources available	☐	☐	☐	

GO-LIVE READINESS

Readiness Item	Complete	Incomplete	N/A	Comments
Implementation date approved	☐	☐	☐	
Help desk available	☐	☐	☐	
Incident reporting process active	☐	☐	☐	
QAPI monitoring plan established	☐	☐	☐	
Post-implementation review scheduled	☐	☐	☐	

Overall Readiness

☐ Ready for Implementation ☐ Ready with Corrective Actions ☐ Not Ready

Required Corrective Actions / Notes _____

Approvals

Project Lead _____ Date _____

Clinical Manager _____ Date _____

Director of Nursing _____ Date _____

Administrator _____ Date _____

AI Oversight Committee(GB) _____ Date _____

AI USER ACCESS AUTHORIZATION FORM

Use this form to authorize, modify, or terminate workforce access to Agency-approved Artificial Intelligence (AI) applications.

Employee Name:		Employee ID:	
Department:		Job Title:	
Supervisor:		Date:	
AI Application:		Vendor:	

Access Request Type ☐ New Access ☐ Modify Access ☐ Remove Access

USER ACCESS LEVEL

Item	Yes	No	Comments
Read Only	☐	☐	
Documentation Support	☐	☐	
Voice Documentation	☐	☐	
Clinical Decision Support	☐	☐	
Administrative Functions	☐	☐	
Quality Reports	☐	☐	
System Administrator	☐	☐	

REQUIRED PREREQUISITES

Item	Yes	No	Comments
AI Orientation Completed	☐	☐	
HIPAA Training Current	☐	☐	
Cybersecurity Training Current	☐	☐	
Annual Competency Completed	☐	☐	
Confidentiality Agreement Signed	☐	☐	
Supervisor Approval Obtained	☐	☐	

ACCESS CONTROLS

Item	Yes	No	Comments
Unique User ID Assigned	☐	☐	
Role-Based Access Verified	☐	☐	
Multi-Factor Authentication Enabled (if applicable)	☐	☐	
Minimum Necessary Access Granted	☐	☐	
Audit Logging Enabled	☐	☐	

User Acknowledgment: I understand that access to Agency-approved AI systems is granted solely for authorized business purposes. I agree to comply with Agency policies, HIPAA requirements, cybersecurity standards, and acceptable use requirements. I understand that I am responsible for protecting my login credentials and reporting any suspected unauthorized access immediately.

Employee Signature: _____ Date: _____

Approvals

Supervisor _____ Date _____

DON (if applicable) _____ Date _____

Administrator, Privacy/Security Officer _____ Date _____

ARTIFICIAL INTELLIGENCE (AI) DISCLOSURE AND PATIENT ACKNOWLEDGMENT

Artificial Intelligence (AI) Disclosure

As part of our commitment to providing high-quality, efficient, and secure healthcare services, our Agency may utilize **Artificial Intelligence (AI)-assisted technology** to support certain administrative and clinical documentation processes associated with your care. The use of **AI** is intended to improve the accuracy, consistency, efficiency, and timeliness of clinical documentation while maintaining compliance with all applicable federal and state laws governing patient privacy and healthcare information.

How AI May Be Used

AI technology may be used to assist authorized Agency personnel with activities including, but not limited to:

- * Drafting clinical documentation based on information entered by licensed clinicians.
- * Assisting with preparation of visit notes
- * Organizing documentation into standardized formats.
- * Improving grammar, spelling, readability, and consistency of documentation.
- * Summarizing clinical information for documentation purposes
- * Assisting with quality assurance and documentation review
- * Supporting administrative workflow and record management.

(AI is not used to independently diagnose medical conditions, prescribe medications, determine treatment plans, or replace the professional judgment of licensed healthcare providers)

Professional Responsibility

Regardless of any AI assistance: Every clinical assessment is performed by qualified healthcare personnel.

All patient care decisions are made solely by licensed healthcare professionals. Every clinical document is reviewed, edited as necessary, approved, and authenticated by the responsible clinician before becoming part of the medical record. The patient's protected health information (PHI) will be safeguarded in accordance with HIPAA and applicable State and Federal regulations.

The clinician remains fully responsible for the accuracy, completeness, and content of the documentation.

AI does not replace the knowledge, judgment, or responsibilities of physicians, nurses, therapists, social workers, or other healthcare professionals.

Privacy and Security

The Agency is committed to protecting your Protected Health Information (PHI). Any AI technology used by the Agency is intended to comply with applicable privacy and security requirements, including: Health Insurance Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health (HITECH) Act, Applicable Centers for Medicare & Medicaid Services (CMS) requirements. Applicable State laws and regulations, and Agency Privacy and Information Security Policies. Reasonable administrative, technical, and physical safeguards are maintained to protect your health information from unauthorized access, use, or disclosure.

Limitations of AI

Artificial Intelligence is a supportive technology and may occasionally generate incomplete or inaccurate information.

For this reason: **AI-generated content is never accepted without human review.** Licensed clinicians verify all information before documentation is finalized. Clinical decisions are never based solely on AI-generated information.

Your Rights

- * Ask questions regarding the Agency's use of AI technology
- * Receive explanations about how your health information is documented
- * Receive healthcare services regardless of whether AI-assisted documentation is utilized
- * Exercise all rights provided under the Agency's Notice of Privacy Practices.

Patient Acknowledgment

I acknowledge that: I have received and read (or had explained to me) this Artificial Intelligence (AI) Disclosure. I understand that AI may be used only as a documentation and administrative support tool. I understand that AI does not replace the professional judgment or clinical decision-making of qualified healthcare professionals. I understand that licensed healthcare personnel remain responsible for my care and for all documentation entered into my medical record. I understand that the Agency is committed to protecting my Protected Health Information in accordance with applicable federal and state privacy laws. I have had the opportunity to ask questions regarding this disclosure.

AUTHORIZATION:

I understand the information provided regarding the possible use of Artificial Intelligence (AI) technology during the provision of my home health services and in the documentation of my care. The authorization is signed on the second page of the Service Agreement, and a copy has been provided to me, or my legal representative. The signed authorization will be part of patient clinical record.

AI DOCUMENTATION REVIEW CHECKLIST

Use this checklist to review AI-assisted clinical or administrative documentation before it becomes part of the legal medical record.

Patient Name:		MRN:	
Clinician:		Review Date:	
Document Type:		AI Application:	

DOCUMENT ACCURACY

Review Item	Yes	No	N/A	Comments
Patient identity verified	☐	☐	☐	
Assessment findings accurate	☐	☐	☐	
Visit date/time correct	☐	☐	☐	
Services performed accurately documented	☐	☐	☐	
Narrative reflects actual care	☐	☐	☐	

CLINICAL REVIEW

Review Item	Yes	No	N/A	Comments
Medication information verified	☐	☐	☐	
Physician orders verified	☐	☐	☐	
Clinical findings supported	☐	☐	☐	
Patient-specific information confirmed	☐	☐	☐	
No unsupported AI content	☐	☐	☐	

DOCUMENTATION QUALITY

Review Item	Yes	No	N/A	Comments
Complete documentation	☐	☐	☐	
Objective language used	☐	☐	☐	
Grammar and spelling reviewed	☐	☐	☐	
No duplicate/generic text	☐	☐	☐	
Documentation consistent with Plan of Care	☐	☐	☐	

COMPLIANCE REVIEW

Review Item	Yes	No	N/A	Comments
Meets CMS documentation requirements	☐	☐	☐	
HIPAA requirements maintained	☐	☐	☐	
OASIS support verified (if applicable)	☐	☐	☐	
Human review completed	☐	☐	☐	
Electronic signature applied	☐	☐	☐	

Overall Review Determination ☐ Approved ☐ Approved After Corrections ☐ Return for Revision

Reviewer Comments / Required Corrections _____

Reviewer Signature

Reviewer: _____ Date: _____

DON (if applicable): _____ Date: _____

AI CLINICAL VALIDATION CHECKLIST

Complete this checklist before implementing or significantly modifying any Artificial Intelligence (AI) application used to support clinical care, documentation, or clinical decision support.

AI Application:		Vendor:	
Version:		Validation Date:	
Department:		Validated By:	

CLINICAL FUNCTIONALITY

Validation Item	Yes	No	N/A	Comments
Clinical purpose defined	☐	☐	☐	
Supports intended workflow	☐	☐	☐	
Supports clinician efficiency	☐	☐	☐	
Does not replace clinical judgment	☐	☐	☐	
Clinical limitations documented	☐	☐	☐	

DOCUMENTATION VALIDATION

Validation Item	Yes	No	N/A	Comments
Documentation accuracy verified	☐	☐	☐	
Patient-specific content maintained	☐	☐	☐	
Medication information validated	☐	☐	☐	
Physician orders accurately reflected	☐	☐	☐	
Grammar and formatting acceptable	☐	☐	☐	
No fabricated or unsupported content	☐	☐	☐	

CLINICAL DECISION SUPPORT

Validation Item	Yes	No	N/A	Comments
Recommendations are advisory only	☐	☐	☐	
Clinician review required	☐	☐	☐	
OASIS support validated (if applicable)	☐	☐	☐	
Clinical findings supported by assessment	☐	☐	☐	
Patient safety risks evaluated	☐	☐	☐	

WORKFLOW & USABILITY AI CLINICAL VALIDATION CHECKLIST

Validation Item	Yes	No	N/A	Comments
Workflow testing completed	☐	☐	☐	
Pilot testing completed (if applicable)	☐	☐	☐	
User Acceptance Testing completed	☐	☐	☐	
Training materials available	☐	☐	☐	
Human oversight process established	☐	☐	☐	

REGULATORY COMPLIANCE

Validation Item	Yes	No	N/A	Comments
CMS Conditions of Participation reviewed	☐	☐	☐	
HIPAA compliance verified	☐	☐	☐	
Agency policy compliance verified	☐	☐	☐	
Documentation standards met	☐	☐	☐	
QAPI monitoring established	☐	☐	☐	

Overall Clinical Validation Decision

☐ Validated for Implementation
 ☐ Validated with Corrective Actions
 ☐ Additional Validation Required
 ☐ Not Validated

Corrective Actions / Reviewer Comments _____

Approvals

Clinical Manager _____ Date _____

Director of Nursing _____ Date _____

Quality Improvement _____ Date _____

Administrator _____ Date _____

AI Oversight Committee(BD) _____ Date _____

AI INCIDENT REPORT FORM

Use this form to report any actual or suspected Artificial Intelligence (AI)-related incident affecting patient care, documentation, privacy, cybersecurity, regulatory compliance, or Agency operations.

Date of Incident:		Time:	
Reported By:		Department:	
AI Application:		Vendor:	
Patient Name (if applicable):		Medical Record #:	

Incident Type (Check all that apply)

Incident Type	Select
AI documentation error	☐
Incorrect AI recommendation	☐
Privacy violation	☐
Cybersecurity incident	☐
Unauthorized AI use	☐
Vendor failure	☐
Data breach	☐
Medication documentation error	☐
OASIS documentation issue	☐
Voice transcription error	☐
Workflow failure	☐
Other:	☐

Incident Description

Describe what occurred, including the sequence of events, systems involved, and any impact on patient care or operations.

Immediate Actions Taken

AI INCIDENT REPORT FORM

Investigation Summary

Corrective Actions

Follow-Up Checklist:

Follow-Up Item	Mark
Patient safety evaluated	☐
Documentation corrected	☐
Privacy Officer notified (if applicable)	☐
Security Officer notified (if applicable)	☐
Vendor notified	☐
QAPI referral completed	☐
Root Cause Analysis completed	☐
Staff education provided	☐
Corrective actions verified	☐

Approvals

Supervisor _____ Date _____

Clinical Manager/DON _____ Date _____

Privacy/Security Officer, Administrator _____ Date _____

QAPI Review Date _____

AI PRIVACY BREACH REPORT FORM

Use this form to report any actual or suspected privacy breach involving an Agency-approved Artificial Intelligence (AI) application or AI-assisted process.

Date Discovered:		Time:	
Reported By:		Department:	
AI Application:		Vendor:	
Patient(s) Affected:		Medical Record #:	

Type of Privacy Incident (Check all that apply)

Incident Type	Select
Unauthorized disclosure of PHI	☐
Unauthorized access to AI system	☐
Use of unapproved AI application	☐
Lost or stolen device	☐
Improper transmission of PHI	☐
Incorrect patient information disclosed	☐
Vendor security/privacy issue	☐
Suspected HIPAA violation	☐
Potential reportable breach	☐
Other: _____	☐

Description of Incident

Information Potentially Disclosed (Describe PHI involved)

AI PRIVACY BREACH REPORT FORM

Immediate Containment Actions

Investigation Findings

Corrective Actions Implemented

Notification & Follow-Up Checklist

Follow-Up Item	Completed
Privacy Officer notified	☐
Administrator notified	☐
Information Security notified (if applicable)	☐
Vendor notified (if applicable)	☐
HIPAA risk assessment completed	☐
Patients notified (if required)	☐
Regulatory notification completed (if required)	☐
QAPI referral completed	☐
Staff re-education completed	☐

Approvals

Privacy Officer _____ Date _____

Information Security Officer _____ Date _____

Administrator _____ Date _____

QAPI Review Date _____

AI ANNUAL COMPETENCY CHECKLIST

Complete annually for all workforce members authorized to use Agency-approved Artificial Intelligence (AI) technologies. This checklist documents annual competency validation and supports the Agency's Quality Assurance and Performance Improvement (QAPI) Program.

Staff Name:		Department:	
Job Title:		Hire Date:	
Supervisor:		Evaluation Date:	
AI Application(s):			

KNOWLEDGE OF AGENCY AI POLICIES

Competency Item	Competent	Needs Improvement	When	Comments
Understands approved uses of AI	☐	☐	☐	
Understands prohibited uses of AI	☐	☐	☐	
Understands human oversight requirements	☐	☐	☐	
Understands documentation standards	☐	☐	☐	
Understands incident reporting procedures	☐	☐	☐	

REGULATORY COMPLIANCE

Competency Item	Competent	Needs Improvement	When	Comments
HIPAA Privacy and Security requirements	☐	☐	☐	
CMS Conditions of Participation awareness	☐	☐	☐	
Agency AI policy compliance	☐	☐	☐	
Privacy and confidentiality maintained	☐	☐	☐	

CLINICAL DOCUMENTATION

Competency Item	Competent	Needs Improvement	When	Comments
Reviews AI-generated documentation	☐	☐	☐	
Verifies medication information	☐	☐	☐	
Verifies physician orders	☐	☐	☐	
Identifies AI errors or hallucinations	☐	☐	☐	
Applies electronic authentication correctly	☐	☐	☐	

Competency Item	Competent	Needs Improvement	When	Comments
Uses approved AI platforms only	☐	☐	☐	
Protects login credentials	☐	☐	☐	
Recognizes phishing/security threats	☐	☐	☐	
Reports suspected security incidents	☐	☐	☐	

COMPETENCY VALIDATION

Competency Item	Competent	Needs Improvement	When	Comments
Successfully completed knowledge assessment	☐	☐	☐	
Demonstrated safe AI use	☐	☐	☐	
Completed annual AI training	☐	☐	☐	
Competent for continued AI access	☐	☐	☐	

Overall Competency Determination

☐ Competent ☐ Competent with Additional Training ☐ Not Yet Competent

Remediation / Education Required

Evaluator Comments

Signatures

Employee _____ Date _____
 Evaluator _____ Date _____
 Clinical Manager _____ Date _____
 Director of Nursing _____ Date _____

AI QUARTERLY AUDIT TOOL

Use this tool to perform quarterly Quality Assurance and Performance Improvement (QAPI) audits of Artificial Intelligence (AI) technologies and AI-assisted processes.

Audit Quarter:		Year:	
Department:		Auditor:	
AI Application:		Vendor:	

DOCUMENTATION QUALITY

Audit Item	Compliant	Non-Compliant	N/A	Comments
AI-assisted documentation accurate	☐	☐	☐	
Patient-specific documentation	☐	☐	☐	
Medication information verified	☐	☐	☐	
Physician orders reflected	☐	☐	☐	
No duplicate/generic documentation	☐	☐	☐	
Documentation authenticated	☐	☐	☐	

REGULATORY COMPLIANCE

Audit Item	Compliant	Non-Compliant	N/A	Comments
CMS documentation requirements met	☐	☐	☐	
HIPAA requirements met	☐	☐	☐	
Human oversight documented	☐	☐	☐	
OASIS support appropriate (if applicable)	☐	☐	☐	
Agency policy followed	☐	☐	☐	

PRIVACY & SECURITY

Audit Item	Compliant	Non-Compliant	N/A	Comments
No unauthorized AI use	☐	☐	☐	
Access controls reviewed	☐	☐	☐	
Audit logs reviewed	☐	☐	☐	
No privacy incidents this quarter	☐	☐	☐	
Cybersecurity controls effective	☐	☐	☐	

STAFF COMPETENCY

AI QUARTERLY AUDIT TOOL

Audit Item	Compliant	Non-Compliant	N/A	Comments
Required training completed	☐	☐	☐	
Annual competency current	☐	☐	☐	
Staff following AI policy	☐	☐	☐	
Incident reporting understood	☐	☐	☐	

QAPI & PERFORMANCE

Audit Item	Compliant	Non-Compliant	N/A	Comments
Corrective actions completed	☐	☐	☐	
Vendor performance acceptable	☐	☐	☐	
Incident trends reviewed	☐	☐	☐	
PIP required?	☐	☐	☐	
Overall AI performance acceptable	☐	☐	☐	

Audit Summary

Overall Result: ☐ Satisfactory ☐ Needs Improvement ☐ Corrective Action Required

Key Findings

Corrective Actions

Performance Improvement Project (PIP) Recommendation

Approvals

Auditor _____ Date _____

Clinical Manager _____ Date _____

Director of Nursing _____ Date _____

QAPI Committee Chair _____ Date _____

Administrator _____ Date _____

AI QAPI MONITORING DASHBOARD

Quarterly Quality Assessment and Performance Improvement (QAPI) monitoring tool for Artificial Intelligence (AI) implementation and oversight.

Quarter:		Year:		Department:	
AI Application:				Vendor:	
Prepared By:		Review Date		QAPI Meeting	

Key Performance Indicators (KPIs)

Indicator	Goal	Current	Previous	Trend	Action Needed
AI Documentation Accuracy	≥98%				
Documentation Error Rate	≤2%				
Privacy Incidents	0				
Cybersecurity Events	0				
Staff AI Training Completion	100%				
Annual Competency Completion	100%				
AI Documentation Audits Passed	≥95%				
Patient Complaints Related to AI	0				
Vendor Performance	Satisfactory				
Corrective Actions Completed	100%				
Performance Improvement Projects (PIPs)	As Needed				

Quarterly Findings

Corrective Actions / Opportunities for Improvement

AI QAPI MONITORING DASHBOARD (Cont'd)

Performance Improvement Project (PIP) Summary

Recommendations for Governing Body

QAPI Committee Review

QAPI Committee Chair _____ Date _____

Director of Nursing(DON) _____ Date _____

Administrator _____ Date _____

Governing Body Review Date _____

AI CORRECTIVE ACTION PLAN (CAP)

Use this form to document corrective actions resulting from AI-related audits, incidents, QAPI reviews, privacy events, security findings, vendor issues, or regulatory deficiencies.

CAP Number:		Date Initiated:	
Department:		AI Application:	
Vendor:		Responsible Manager:	
Source of Finding:		Priority: High/Medium/ Low	

Problem Statement

Root Cause Analysis

Immediate Corrective Actions

Corrective Action Tracking

Action Item	Responsible Person	Due Date	Completion Date	Status

Effectiveness Review

Follow-Up Monitoring

QAPI Committee Comments

Final Disposition

☐ Closed ☐ Continue Monitoring ☐ Escalate to Performance Improvement Project (PIP)

Approvals

Responsible Manager _____ Date _____

Director of Nursing (DON) _____ Date _____

QAPI Committee Chair _____ Date _____

Administrator _____ Date _____

AI STAFF TRAINING

EDUCATION • COMPETENCY • SAFE USE • EXCELLENCE IN CARE

EMPOWERING STAFF. ENHANCING CARE. IMPROVING OUTCOMES.



OUR GOAL

Use Artificial Intelligence safely, ethically, and responsibly to support accurate documentation, improve efficiency, ensure compliance, and deliver high-quality, patient-centered care.

AI IS A TOOL. YOU ARE THE EXPERT.

- AI supports your work.
- You make the decisions.
- Human judgment and oversight are always required.



1. AI BASICS

- What is AI?
- Types of AI in healthcare
- Benefits and limitations
- AI does not replace professional judgment



2. APPROPRIATE USE

- Approved AI tools and systems
- Permitted uses:
 - Documentation support
 - Clinical decision support
 - Patient education
 - Administrative tasks
- Prohibited uses:
 - Diagnosing without evaluation
 - Replacing assessments
 - Creating false documentation
 - Sharing PHI with public AI tools



3. DOCUMENTATION & CLINICAL RECORD INTEGRITY

- Accurate, clear, complete, and timely
- AI-generated content must be reviewed and verified
- Do not copy/paste without clinical justification
- Individualized to each patient
- Authenticate all documentation
- Detect and correct AI errors (hallucinations)



7. DOCUMENTATION STANDARDS

- Follow all agency and Medicare requirements
- Support documentation with clinical evidence
- Maintain audit-ready records



8. QUALITY ASSESSMENT & PERFORMANCE IMPROVEMENT (QAPI)

- Monitor AI use and outcomes
- Review documentation quality
- Track errors and trends
- Implement improvements



9. FRAUD, WASTE & ABUSE PREVENTION

- Accurate documentation
- No upcoding or misrepresentation
- Bill only for services actually provided
- Report concerns



10. EMPLOYEE CODE OF CONDUCT

- Act with integrity
- Be ethical and professional
- Respect patients and colleagues
- Report unethical or inappropriate AI use



11. PATIENT RIGHTS & CONFIDENTIALITY

- Respect privacy and dignity
- Provide clear information
- Support informed decisions
- Maintain confidentiality at all times



12. HUMAN OVERSIGHT

- You are responsible for all decisions and documentation
- Verify AI recommendations
- Use clinical judgment
- When in doubt, escalate



13. EDUCATION & COMPETENCY

- Complete initial training
- Pass competency validation
- Complete annual education
- Stay informed on updates
- Competency = Confidence + Safety



14. INCIDENT REPORTING

- Report AI errors, data breaches, or policy violations
- Use AI Incident Report Form
- Timely reporting improves safety and prevents harm

AI IN ACTION



Assists with documentation and summaries



Supports clinical decision-making with evidence



Improves scheduling and care coordination



Enhances quality and compliance



Helps deliver better patient outcomes



SAFE AI USE. STRONGER CARE. BETTER OUTCOMES.

Together, we use technology to enrich care, empower staff, and improve lives.

