AMERICAN MEDICAL ASSOCIATION HOUSE OF DELEGATES

Resolution: (Assigned by HOD)
(A-25)

Introduced by: Private Practice Physician Section

Subject: Grace Period for Timely Filing Due to Technology Failures Regardless of Cause

Referred to: Reference Committee (Assigned by HOD)

Whereas, there is a lag period between when a claim is submitted and when it is acted upon for many payers despite timely filing laws in many states; and

Whereas, for months after the Change Healthcare cyber-event, claims were not being acted upon by payers using this clearinghouse; and

Whereas, some insurers, even those that are subsidiaries of United Healthcare, did not create a grace period for timely filing despite the Change Healthcare cyber-event; and

Whereas, having an all-payer extended grace period would assist practices destabilized by the Change Healthcare cyber-event and would strengthen the healthcare economy by aiding medical practices still weakened by the Covid pandemic to recover financially from the cyber-event; therefore be it

RESOLVED, that our American Medical Association advocate for a two-year grace period from the date of a claims processing failure, allowing payers to resolve claims before denying them based on a “timely filing limit” (Directive to Take Action).

Fiscal Note: (Assigned by HOD)

Received:

RELEVANT AMA POLICY

Ransomware and Electronic Health Records D-478.960

1. Our American Medical Association acknowledges that healthcare data interruptions are especially harmful due to potential physical harm to patients and calls for prosecution to the fullest extent of the law for perpetrators of ransomware and any other malware on independent physicians and their practices, healthcare organizations, or other medical entities involved in providing direct and indirect care to patients.
2. Our AMA will:
    a. advocate for federal legislation which provides for the prosecution of perpetrators of ransomware and any other malware on any and all healthcare entities, involved in direct and indirect patient care, to the fullest extent of the law;
    b. encourage health care facilities and integrated networks that are under threat of ransomware attacks to upgrade their cybersecurity and to back up data in a robust and timely fashion;
    c. advocate that the security of protected healthcare information be considered as an integral part of national cybersecurity protection; and
    d. seek inclusion of federal cybersecurity resources allocated to physician practices, hospitals, and health care entities sufficient to protect the security of the patients they serve, as part of infrastructure legislation.

Citation: Res. 210, A-21; Reaffirmed: Res. 241, A-24

Assessing the Intersection Between AI and Health Care H-480.931

Augmented Intelligence Development, Deployment, and Use in Health Care

1. General Governance
    a. Health care AI must be designed, developed, and deployed in a manner which is ethical, equitable, responsible, accurate, transparent, and evidence-based.
    b. Use of AI in health care delivery requires clear national governance policies to regulate its adoption and utilization, ensuring patient safety, and mitigating inequities. Development of national governance policies should include interdepartmental and interagency collaboration.
    c. Compliance with national governance policies is necessary to develop AI in an ethical and responsible manner to ensure patient safety, quality, and continued access to care. Voluntary agreements or voluntary compliance is not sufficient.
    d. AI systems should be developed and evaluated with a specific focus on mitigating bias and promoting health equity, ensuring that the deployment of these technologies does not exacerbate existing disparities in health care access, treatment, or outcomes.
    e. Health care AI requires a risk-based approach where the level of scrutiny, validation, and oversight should be proportionate to the overall potential of disparate harm and consequences the AI system might introduc [See also Augmented Intelligence in Health Care H-480.939 at (1)]
    f. AI risk management should minimize potential negative impacts of health care AI systems while providing opportunities to maximize positive impacts.

g. Clinical decisions influenced by AI must be made with specified qualified human intervention points during the decision-making process. A qualified human is defined as a licensed physician with the necessary qualifications and training to independently provide the same medical service without the aid of AI. As the potential for patient harm increases, the point in time when a physician should utilize their clinical judgment to interpret or act on an AI recommendation should occur earlier in the care plan. With few exceptions, there generally should be a qualified human in the loop when it comes to medical decision making capable of intervening or overriding the output of an AI model.
h. Health care practices and institutions should not utilize AI systems or technologies that introduce overall or disparate risk that is beyond their capabilities to mitigate. Implementation and utilization of AI should avoid exacerbating clinician burden and should be designed and deployed in harmony with the clinical workflow and, in institutional settings, consistent with AMA Policy H-225.940 - Augmented Intelligence and Organized Medical Staff.
i. Medical specialty societies, clinical experts, and informaticists are best positioned and should identify the most appropriate uses of AI-enabled technologies relevant to their clinical expertise and set the standards for AI use in their specific domain. [See Augmented Intelligence in Health Care H-480.940 at (2)]

2. When to Disclose: Transparency in Use of Augmented Intelligence-Enabled Systems and Technologies That Impact Medical Decision Making at the Point of Care
    a. Decisions regarding transparency and disclosure of the use of AI should be based upon a risk- and impact-based approach that considers the unique circumstance of AI and its use case. The need for transparency and disclosure is greater where the performance of an AI-enabled technology has a greater risk of causing harm to a patient.
        i. AI disclosure should align and meet ethical standards or norms.
        ii. Transparency requirements should be designed to meet the needs of the end users. Documentation and disclosure should enhance patient and physician knowledge without increasing administrative burden.
        iii. When AI is used in a manner which impacts access to care or impacts medical decision making at the point of care, that use of AI should be disclosed and documented to both physicians and/or patients in a culturally and linguistically appropriate manner. The opportunity for a patient or their caregiver to request additional review from a licensed clinician should be made available upon request.
        iv. When AI is used in a manner which directly impacts patient care, access to care, medical decision making, or the medical record, that use of AI should be documented in the medical record.
    b. AI tools or systems cannot augment, create, or otherwise generate records, communications, or other content on behalf of a physician without that physician’s consent and final review.
    c. When AI or other algorithmic-based systems or programs are utilized in ways that impact patient access to care, such as by payors to make claims determinations or set coverage limitations, use of those systems or programs must be disclosed to impacted parties.
    d. The use of AI-enabled technologies by hospitals, health systems, physician practices, or other entities, where patients engage directly with AI, should be clearly disclosed to patients at the beginning of the encounter or interaction with the AI-enabled technology. Where patient-facing content is generated by AI, the use of AI in generating that content should be disclosed or otherwise noted within the content.

3. What to Disclose: Required Disclosures by Health Care Augmented Intelligence-Enabled Systems and Technologies
    a. When AI-enabled systems and technologies are utilized in health care, the following information should be disclosed by the AI developer to allow the purchaser and/or user (physician) to appropriately evaluate the system or technology prior to purchase or utilization:
        i. Regulatory approval status.
        ii. Applicable consensus standards and clinical guidelines utilized in design, development, deployment, and continued use of the technology.
        iii. Clear description of problem formulation and intended use accompanied by clear and detailed instructions for use.
        iv. Intended population and intended practice setting.
        v. Clear description of any limitations or risks for use, including possible disparate impact.
        vi. Description of how impacted populations were engaged during the AI lifecycle.
        vii. Detailed information regarding data used to train the model:
            1. Data provenance.
            2. Data size and completeness.
            3. Data timeframes.
            4. Data diversity.
            5. Data labeling accuracy.
        viii. Validation Data/Information and evidence of:
            1. Clinical expert validation in intended population and practice setting and intended clinical outcomes.
            2. Constraint to evidence-based outcomes and mitigation of “hallucination”/“confabulation” or other output error.
            3. Algorithmic validation.
            4. External validation processes for ongoing evaluation of the model performance, e.g., accounting for AI model drift and degradation.
            5. Comprehensiveness of data and steps taken to mitigate biased outcomes.
            6. Other relevant performance characteristics, including but not limited to performance characteristics at peer institutions/similar practice settings.
            7. Post-market surveillance activities aimed at ensuring continued safety, performance, and equity.
        ix. Data Use Policy:
            1. Privacy.
            2. Security.
            3. Special considerations for protected populations or groups put at increased risk.
        x. Information regarding maintenance of the algorithm, including any use of active patient data for ongoing training.
        xi. Disclosures regarding the composition of design and development team, including diversity and conflicts of interest, and points of physician involvement and review.
    b. Purchasers and/or users (physicians) should carefully consider whether or not to engage with AI-enabled health care technologies if this information is not disclosed by the developer. As the risk of AI being incorrect increases risks to patients (such as with clinical applications of AI that impact medical decision

making), disclosure of this information becomes increasingly important. [See also Augmented Intelligence in Health Care H-480.939]

4. Generative Augmented Intelligence
    a. Generative AI should: (a) only be used where appropriate policies are in place within the practice or other health care organization to govern its use and help mitigate associated risks; and (b) follow applicable state and federal laws and regulations (e.g., HIPAA-compliant Business Associate Agreement).
    b. Appropriate governance policies should be developed by health care organizations and account for and mitigate risks of:
        i. Incorrect or falsified responses; lack of ability to readily verify the accuracy of responses or the sources used to generate the response.
        ii. Training data set limitations that could result in responses that are out of date or otherwise incomplete or inaccurate for all patients or specific populations.
        iii. Lack of regulatory or clinical oversight to ensure performance of the tool.
        iv. Bias, discrimination, promotion of stereotypes, and disparate impacts on access or outcomes.
        v. Data privacy.
        vi. Cybersecurity.
        vii. Physician liability associated with the use of generative AI tools.
    c. Health care organizations should work with their AI and other health information technology (health IT) system developers to implement rigorous data validation and verification protocols to ensure that only accurate, comprehensive, and bias managed datasets inform generative AI models, thereby safeguarding equitable patient care and medical outcomes. [See Augmented Intelligence in Health Care H-480.940 at (3)(d)]
    d. Use of generative AI should incorporate physician and staff education about the appropriate use, risks, and benefits of engaging with generative AI. Additionally, physicians and healthcare organizations should engage with generative AI tools only when adequate information regarding the product is provided to physicians and other users by the developers of those tools.
    e. Clinicians should be aware of the risks of patients engaging with generative AI products that produce inaccurate or harmful medical information (g., patients asking chatbots about symptoms) and should be prepared to counsel patients on the limitations of AI-driven medical advice.
5. Physician Liability for Use of Augmented Intelligence-Enabled Technologies
    a. Current AMA policy states that liability and incentives should be aligned so that the individual(s) or entity(ies) best positioned to know the AI system risks and best positioned to avert or mitigate harm do so through design, development, validation, and implementation. [See Augmented Intelligence in Health Care H-480.939]
        i. Where a mandated use of AI systems prevents mitigation of risk and harm, the individual or entity issuing the mandate must be assigned all applicable liability.
        ii. Developers of autonomous AI systems with clinical applications (screening, diagnosis, treatment) are in the best position to manage issues of liability arising directly from system failure or misdiagnosis and must accept this liability with measures such as maintaining appropriate medical liability insurance and in their agreements with users.
        iii. Health care AI systems that are subject to non-disclosure agreements concerning flaws, malfunctions, or patient harm (referred to as gag

clauses) must not be covered or paid and the party initiating or enforcing the gag clause assumes liability for any harm.

b. When physicians do not know or have reason to know that there are concerns about the quality and safety of an AI-enabled technology, they should not be held liable for the performance of the technology in question.
c. Liability protections for physicians using AI-enabled technologies should align with both current and future AMA medical liability reform policies.

6. Data Privacy and Augmented Intelligence
    a. Entity Responsibility:
        i. Entities, e.g., AI developers, should make information available about the intended use of generative AI in health care and identify the purpose of its use. Individuals should know how their data will be used or reused, and the potential risks and benefits.
        ii. Individuals should have the right to opt-out, update, or request deletion of their data from generative AI tools. These rights should encompass AI training data and disclosure to other users of the tool.
        iii. Generative AI tools should not reverse engineer, reconstruct, or reidentify an individual's originally identifiable data or use identifiable data for nonpermitted uses, e.g., when data are permitted to conduct quality and safety evaluations. Preventive measures should include both legal frameworks and data model protections, e.g., secure enclaves, federated learning, and differential privacy.
    b. User Education:
        i. Users should be provided with training specifically on generative AI. Education should address:
            1. Legal, ethical, and equity considerations.
            2. Risks such as data breaches and re-identification.
            3. Potential pitfalls of inputting sensitive and personal data.
            4. The importance of transparency with patients regarding the use of generative AI and their data.

[See H-480.940, Augmented Intelligence in Health Care, at (4) and (5)]

7. Augmented Intelligence Cybersecurity
    a. AI systems must have strong protections against input manipulation and malicious attacks.
    b. Entities developing or deploying health care AI should regularly monitor for anomalies or performance deviations, comparing AI outputs against known and normal behavior.
    c. Independent of an entity's legal responsibility to notify a health care provider or organization of a data breach, that entity should also act diligently in identifying and notifying the individuals themselves of breaches that impact their personal information.
    d. Users should be provided education on AI cybersecurity fundamentals, including specific cybersecurity risks that AI systems can face, evolving tactics of AI cyber attackers, and the user's role in mitigating threats and reporting suspicious AI behavior or outputs.
8. Mitigating Misinformation in AI-Enabled Technologies
    a. AI developers should ensure transparency and accountability by disclosing how their models are trained and the sources of their training dat Clear disclosures are necessary to build trust in the accuracy and reliability of the information produced by AI systems.
    b. Algorithms should be developed to detect and flag potentially false and misleading content before it is widely disseminated.

c. Developers of AI should have mechanisms in place to allow for reporting of mis- and disinformation generated or propagated by AI-enabled systems.
d. Developers of AI systems should be guided by policies that emphasize rigorous validation and accountability for the content their tools generate, and, consistent with AMA Policy H-480.939(7), are in the best position to manage issues of liability arising directly from system failure or misdiagnosis and must accept this liability with measures such as maintaining appropriate medical liability insurance and in their agreements with users.
e. Academic publications and journals should establish clear guidelines to regulate the use of AI in manuscript submissions. These guidelines should include requiring the disclosure that AI was used in research methods and data collection, requiring the exclusion of AI systems as authors, and should outline the responsibility of the authors to validate the veracity of any referenced content generated by AI.
f. Education programs are needed to enhance digital literacy, helping individuals critically assess the information they encounter online, particularly in the medical field where mis- and disinformation can have severe consequences.

9. Payor Use of Augmented Intelligence and Automated Decision-Making Systems
    a. Use of automated decision-making systems that determine coverage limits, make claim determinations, and engage in benefit design should be publicly reported, based on easily accessible evidence-based clinical guidelines (as opposed to proprietary payor criteria), and disclosed to both patients and their physician in a way that is easy to understand.
    b. Payors should only use automated decision-making systems to improve or enhance efficiencies in coverage and payment automation, facilitate administrative simplification, and reduce workflow burdens. Automated decision-making systems should never create or exacerbate overall or disparate access barriers to needed benefits by increasing denials, coverage limitations, or limiting benefit offerings. Use of automated decision-making systems should not replace the individualized assessment of a patient's specific medical and social circumstances and payors' use of such systems should allow for flexibility to override automated decisions. Payors should always make determinations based on particular patient care needs and not base decisions on algorithms developed on "similar" or "like" patients.
    c. Payors using automated decision-making systems should disclose information about any algorithm training and reference data, including where data were sourced and attributes about individuals contained within the training data set (e.g., age, race, gender). Payors should provide clear evidence that their systems do not discriminate, increase inequities, and that protections are in place to mitigate bias.
    d. Payors using automated decision-making systems should identify and cite peer-reviewed studies assessing the system's accuracy measured against the outcomes of patients and the validity of the system's predictions.
    e. Any automated decision-making system recommendation that indicates limitations or denials of care, at both the initial review and appeal levels, should be automatically referred for review to a physician (a) possessing a current and valid non-restricted license to practice medicine in the state in which the proposed services would be provided if authorized and (b) be of the same specialty as the physician who typically manages the medical condition or disease or provides the health care service involved in the request prior to issuance of any final determination. Prior to issuing an adverse determination, the treating physician must have the opportunity to discuss the medical necessity

of the care directly with the physician who will be responsible for determining if the care is authorized.

f. Individuals impacted by a payor's automated decision-making system, including patients and their physicians, must have access to all relevant information (including the coverage criteria, results that led to the coverage determination, and clinical guidelines used).
g. Payors using automated decision-making systems should be required to engage in regular system audits to ensure use of the system is not increasing overall or disparate claims denials or coverage limitations, or otherwise decreasing access to care. Payors using automated decision-making systems should make statistics regarding systems' approval, denial, and appeal rates available on their website (or another publicly available website) in a readily accessible format with patient population demographics to report and contextualize equity implications of automated decisions. Insurance regulators should consider requiring reporting of payor use of automated decision-making systems so that they can be monitored for negative and disparate impacts on access to care. Payor use of automated decision-making systems must conform to all relevant state and federal laws.

Citation: BOT Rep. 1, I-24

Indemnity for Breaches in Electronic Health Record Cybersecurity D-315.977

Our AMA will advocate for indemnity or other liability protections for physicians whose electronic health record data and other electronic medical systems become the victim of security compromises.

Citation: Res. 221, I-15