RBMA | Radiology Business Management Association

PO BOX 1636
Evansville, IN 47706-0038

Direct: 703-621-3359
Main: 888-224-7262
Fax: 703-621-3356
www.rbma.org

February 28, 2025

Department of Health & Human Services
Office of the Secretary
200 Independence Ave SW
Washington DC 20201

Re: HHS-OCR-2024-0020
RIN Number 0945-AA22

The Radiology Business Management Association (RBMA) appreciates the opportunity to submit comments to the Department of Health and Human Services, Office of Civil Rights (HHS) regarding the notice of proposed rulemaking (NPRM) titled HIPAA Security Rule to Strengthen the Cybersecurity of Electronic Protected Health Information.

Established in 1968, RBMA is a professional association that consists of over 2,200 radiology practice business leaders who represent over 800 radiology practices in all 50 states. This includes diagnostic radiology, interventional radiology, nuclear medicine, Independent Diagnostic Testing Facilities (IDTFs) and radiation oncology.

RBMA is the trusted partner of radiology professionals, advancing the industry and broadening our members' capacity to provide superior patient experiences. RBMA endorses the following core values in support of its vision and mission: Community, Innovation, Collaboration and Inclusion.

RBMA is committed to protecting our patients' private health information. We support reasonable measures to ensure this protection. However, many of the additional requirements outlined in the proposed rule could be cost prohibitive without generating a commensurate level of additional protection for individual patients, their providers or business associates.

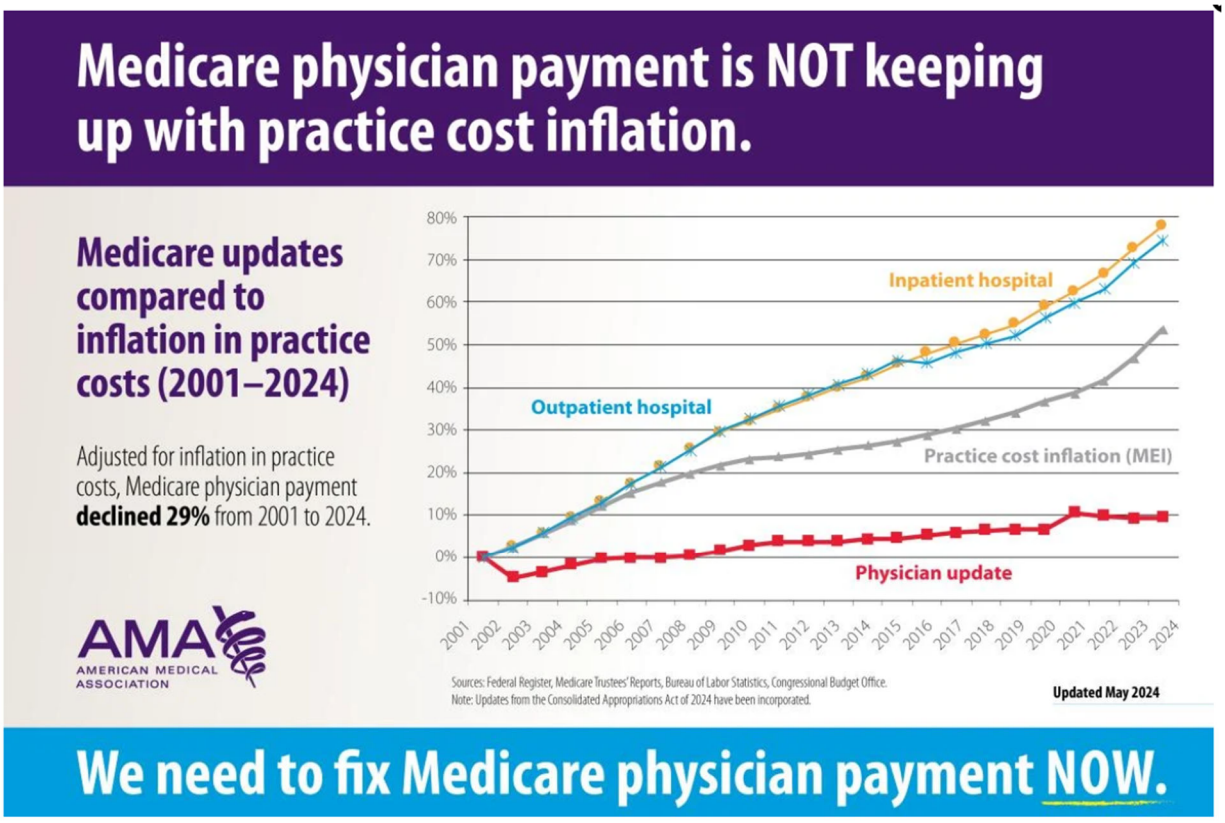
Today Healthcare providers in the United States must comply with a variety of

federal regulations to ensure patient safety, privacy, and the integrity of healthcare services. Although not an exhaustive list of all regulations, the list below illustrates the complexity and burden radiology groups must navigate:

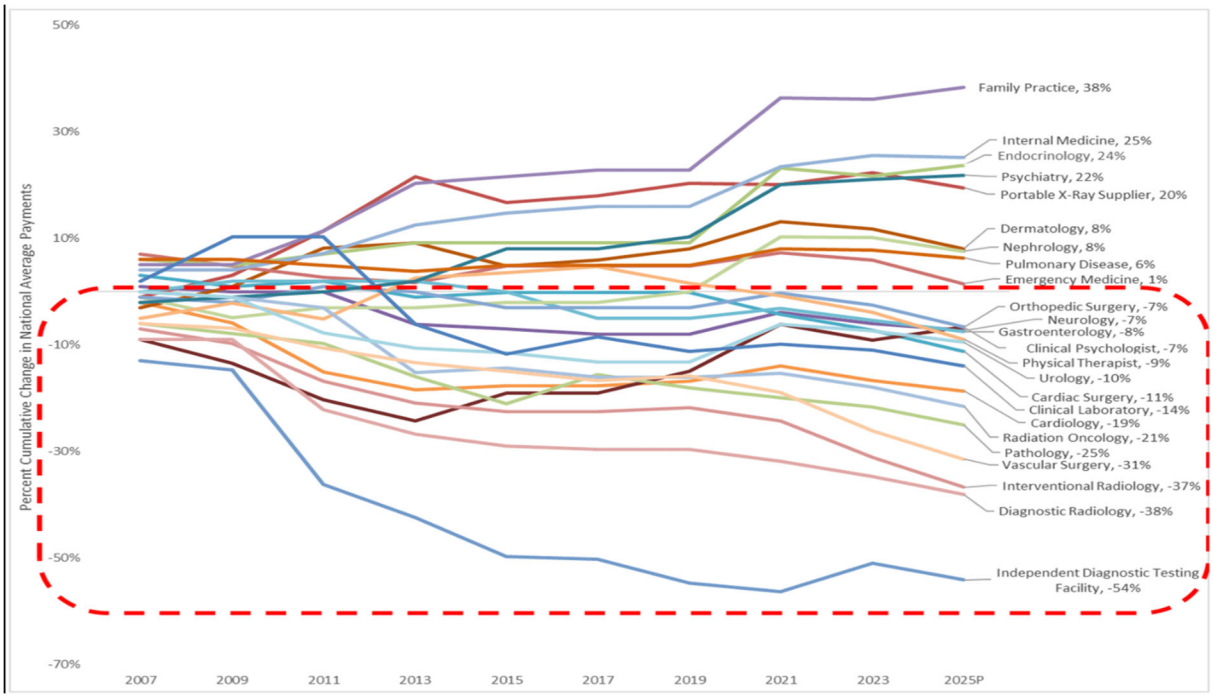
Health Insurance Portability and Accountability Act (HIPAA)
Health Information Technology for Economic and Clinical Health (HITECH) Act
Emergency Medical Treatment and Labor Act (EMTALA)
False Claims Act
Criminal Health Care Fraud Statute
Beneficiary Inducements CMP
Exclusion Authorities
Civil Monetary Penalty Authorities
OSHA
Patient Safety and Quality Improvement Act
Anti-Kickback Statute (AKS)
Physician Self-Referral Law (Stark Law)
Affordable Care Act (ACA)
21st Century Cures Act
Medicare Access and CHIP Reauthorization Act of 2015
No Surprises Act
Mammography Quality Standards Act
Physician Payments and Sunshine Act
Information Blocking Rule
Interoperability and Patient Access Final Rule
Clinical Laboratory Improvement Amendments

The new HIPAA Security Rule Requirements will be particularly burdensome for all physicians, but especially for those in private practice radiology.

Over the past 15 years, physicians have faced significant year-over-year cuts to their reimbursements, while the costs of running a practice have consistently risen. The graphic below, prepared by the American Medical Association, illustrates how physician reimbursement (shown in the red line) has not increased since 2001 according to the Medicare Physician Fee Schedule. When adjusted for inflation, this represents a 29% decrease in reimbursement. Additionally, the grey line highlights that physician reimbursement has not kept pace with the cost of inflation.



We apologize for the complexity of this graphic below, but it underscores the significant reimbursement cuts that Radiology has faced compared to other medical specialties. Prepared by the Outpatient Endovascular and Interventional Society, this graphic shows that from 2007 to the present, Interventional Radiology has experienced a 37% decrease in reimbursement, Diagnostic Radiology a 38% decrease, and Independent Diagnostic Testing Facilities a 54% decrease.



Private practice radiology groups operate on very limited budgets, and the expense associated with implementing this new rule's requirements will be substantial. We understand that HHS estimated that in the first year of implementing the proposed regulatory changes, regulated entities would incur approximately $ 4.655 billion in cost, while plan sponsors would incur about $ 4.659 billion.

This significant increase in costs is anticipated due to the new requirements such as conducting a Security Rule audit, verifying that business associates and subcontractors are compliant with technical safeguards, further deploying multi-factor authentication, conducting penetration testing annually, segmenting networks, disabling network ports, updating all documents and policies and procedures for each organization, workforce training and revisions to business associate agreements.

Additional regulations like the items listed above will likely lead to further consolidation in the healthcare industry, which, as we know, drives up the cost of healthcare. Small, independent radiology groups simply cannot afford to implement such measures.

RBMA below highlights concerns with the proposed rule:

Remove the distinction between "required" and "addressable" implementation specifications and make all implementation specifications required with specific limited exceptions.

RBMA respectfully requests that HHS refer to reasonable measures that are proportionate to the entity's size, resources, risk of exposure and scope of patient information. A one-size- fits all approach will significantly penalize smaller radiology practices that do not have the Information Technology (IT) resources and income to comply with the new requirements. From a practical standpoint RBMA educates their members to practice Cyber Hygiene:

1. Multi-Factor Authentication (MFA)
2. Encryption of all emails with ePHI
3. Network Patching
4. Least Privilege
5. Vendor Vetting
6. Vulnerability Scanning and Penetration Testing
7. Backups
8. Incident Response Plan

The proposed rule aims to update or clarify many definitions where ambiguity exists and or technological advancements have occurred resulting in modifying the meaning. One specific example redefines what is considered a "security incident". HHS is proposing to modify the definition of a security incident to include any attempted or successful unauthorized access, use, disclosure, modification or destruction of information.

RBMA respectfully requests that HHS reconsider the definition, specifically regarding the inclusion of "attempted" unauthorized access.

Most radiology groups have implemented robust processes to mitigate many of these attempts, including firewalls, anti-virus software, monitored detection analysis, multi-factor authentication, and ongoing employee training. These tools have effectively prevented unauthorized access attempts, functioning as designed.

Requiring the tracking, recording, and reporting of these unsuccessful attempts would be overly burdensome and costly. We believe that the current measures in place sufficiently address the issue without the need for additional reporting requirements.

The proposed rules adds specific compliance time periods to many existing requirements.

RBMA respectfully requests that proportionality be considered when implementing the time frames noted in the proposed rule.

For example, the proposed rule requires radiology groups to have written procedures on how they intend to restore the loss of certain relevant clinical information systems and electronic protected health information (ePHI) within 72 hours of experiencing the loss. The systems and processes used by radiology groups for backing up clinical systems and ePHI are diverse, including methods such as tape, cloud, or fixed offsite storage. Each method varies in sophistication and cost.

Given these variations, the proposed 72-hour restoration time frame may not be achievable for all groups. We believe that a more proportional approach, considering the specific backup methods and their associated complexities, would be more practical and less burdensome.

The proposed rule also requires business associates to notify covered entities and subcontractors upon activation of their contingency plans without unreasonable delay, but no later than 24 hours after activation.
AND
The proposed rule is also requiring business associates verify at least once every 12 months that they have deployed technical safeguards required by the Security Rule to protect ePHI, that they have created a network map and technology asset inventory that includes the radiology group in their analysis and have documented a risk analysis that meets the standards set forth in the rule.

RBMA respectfully requests that this requirement be phased in over time and implemented as Business Associate Agreements (BAAs) expire and/or renew.

As previously stated, radiology groups are under significant financial pressure after facing years of reimbursement cuts while the cost of operating our clinics has increased. Complying with this requirement would necessitate engaging legal services, resulting in expensive renegotiations of existing contracts.

We believe a phased implementation approach would alleviate some of the financial burdens and allow radiology groups to adapt effectively while maintaining fiscal stability

The proposed rule additionally requires the development and revision of both a technology asset inventory and a network map that illustrates the movement of ePHI throughout the regulated entity's electronic information system(s) on an ongoing basis, but at least once every 12 months and in response to a change in the regulated entity's environment or operations that may affect ePHI.

RBMA is concerned that requiring radiology organizations to comply with this requirement would be overly burdensome and costly. The life cycle of a radiology exam is complex and requires seamless communication between physicians, their organizations, their electronic medical records systems, and numerous third parties and vendors such as patient-facing systems, radiology information systems, PACS systems, revenue cycle management systems, payer authorization and claims adjudication systems, integration services, decision support tools, etc.

Every step in the radiology workflow involves movement of ePHI—from ordering the exam and scheduling it with the patient, to performing the exam and acquiring the images, then adding the images to the radiologists' worklist for interpretation and dictation into a detailed report, and finally delivering the results to the referring provider. Each step is crucial for patient care and ensuring accurate diagnosis and enabling the business of medicine to proceed efficiently and at scale.

RBMA recommends that providers seek assurances through Business Associate Agreements (BAAs) that the entities they exchange electronic protected health information (ePHI) with are meeting the requirements set forth in this legislation and attest to the same.

In addition to the above, RBMA respectfully requests that HHS consider any organization that has undergone the process of SOC or HITrust certification, or is an Department of Health and Human Services, Assistant Secretary for Technology Policy (ASTP) recognized "certified health IT" vendor as compliant with these regulations.

In summary, RBMA urges the Department of Health and Human Services (HHS) to consider the significant financial and operational burdens that the proposed rule would impose on private practice radiology groups. The estimated costs of compliance are substantial, and the new requirements could lead to further consolidation in the healthcare industry, driving up costs and disadvantaging smaller, independent practices.

RBMA highlights several key concerns and recommendations:

1. **Proportional Measures**: Implement reasonable measures proportionate to the entity's size, resources, risk of exposure, and scope of patient information.
2. **Cyber Hygiene Practices**: Encourage practices such as Multi-Factor Authentication (MFA), encryption, network patching, least privilege, vendor vetting, vulnerability scanning, backups, and incident response planning.
3. **Definition of Security Incident**: Remove the inclusion of "attempted" unauthorized access in the definition of a security incident.
4. **Proportional Time Frames**: Consider the diverse methods used by radiology groups for backing up clinical systems and ePHI when setting restoration time frames.
5. **Phased Implementation**: Phase in new requirements over time as Business Associate Agreements (BAAs) expire and/or renew.
6. **SOC and HiTrust Certification**: Recognize organizations that have undergone SOC or HiTrust certification as compliant with the new regulations.
7. **ASTP Certified Health IT vendor**: Recognize vendors that have obtained and maintain the Certified Health IT vendor status as compliant with the new regulations.
8. **Non-Certified Health IT vendor**: For those health IT vendors who remain uncertified, require that they attest to compliance with "information blocking" and "privacy rule" requirements. Create and publish a public facing database of non-certified health IT vendors who have provided attestations and maintain SOC and/or HiTrust Certifications to enable radiology practices to have awareness and self-select vendors meeting these standards.

We believe these adjustments will help mitigate the financial impact on radiology groups and ensure that patient care remains uncompromised while still ensuring the ongoing security of ePHI for all our patients.

Thank you for your consideration.

Pete Moffatt	Jessica Struve	Linda Wilgus
President	Co-Executive Director	Co – Executive Director