HIPAA AND PERMITTED DISCLOSURES OF PROTECTED HEALTH INFORMATION (PHI)

Purpose of risk management recommendations

OMIC regularly analyzes its claims experience to determine loss prevention measures that our insured ophthalmologists can take to reduce the likelihood of professional liability lawsuits. OMIC policyholders are not required to implement risk management recommendations. Rather, physicians should use their professional judgment in determining the applicability of a given recommendation to their particular patients and practice situation. These loss prevention documents may refer to clinical care guidelines such as the American Academy of Ophthalmology's *Preferred Practice Patterns*, peer-reviewed articles, or to federal or state laws and regulations. However, our risk management recommendations do not constitute the standard of care nor do they provide legal advice. Consult an attorney if legal advice is desired or needed. Information contained here is not intended to be a modification of the terms and conditions of the OMIC professional and limited office premises liability insurance policy. Please refer to the OMIC policy for these terms and conditions.

Version Date: 5/6/2024

RISK ISSUE

HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) **Privacy, Security, and Breach Notification Rules** protect the privacy and security of health information and give patients rights to their health information. HIPAA establishes standards to safeguard the protected health information (PHI) that you hold if you're one of these covered entities or their business associate:

- Health plan
- Health care clearinghouse
- Health care provider

Who enforces HIPAA Rules?

The Department of Health and Human Services (HHS) Office for Civil Rights (OCR) enforces the HIPAA Privacy, Security, and Breach Notification Rules. Violations may result in civil monetary penalties. In some cases, criminal penalties enforced by the U.S. Department of Justice may apply. Common violations include:

- Unpermitted PHI use and disclosure
- Use or disclosure of more than the minimum necessary PHI

- Lack of PHI safeguards
- Lack of administrative, technical, or physical safeguards for PHI that is created, processed, stored, or transmitted electronically (ePHI)
- Lack of patients' access to their PHI

Learn more about the HHS HIPAA Enforcement, including actual case examples.

BACKGROUND

PRIVACY RULE

The Privacy Rule protects your patients' PHI while letting you securely exchange information to coordinate your patients' care. The Privacy Rule also gives patients the right to:

- Examine and get a copy of their medical records, including an electronic copy records
- Request corrections to their medical records
- Restrict their health plan's access to information about treatments they paid for in cash

PHI

The Privacy Rule protects PHI that you hold or transmit in any form, including electronic, hard copy, or oral. PHI includes information about:

- Common identifiers, such as name, address, birth date, and social security number (SSN)
- The patient's past, present, or future physical or mental health condition
- Health care you provide to the patient
- The past, present, or future payment for health care you provide to the patient

Requirements

The Privacy Rule requires you to:

- Notify patients about their privacy rights and how you use their information
- Adopt privacy procedures and train employees to follow them
- Assign an individual to make sure you're adopting and following privacy procedures
- Secure patient records containing PHI so they aren't readily available to those who don't need to see them

Sharing Information with Other Health Care Professionals

To coordinate your patient's care with other providers, the Privacy Rule lets you:

- Share information with doctors, hospitals, and ambulances for treatment, payment, and health care operations, even without a signed consent form from the patient
- Share information about an incapacitated patient if you believe it's in your patient's best interest
- Use health information for research purposes

- Use email, phone, or fax machines to communicate with other health care professionals and with patients, as long as you use safeguards

Sharing Patient Information with Family Members & Others

Unless a patient objects, the Privacy Rule lets you:

- Give information to a patient's family, friends, or anyone else the patient identifies as involved in their care
- Give information about the patient's general condition or location to a patient's family member or anyone responsible for the patient's care
- Include basic information in a hospital directory, such as the patient's phone and room number
- Give information about a patient's religious affiliation to clergy members

Incidental Disclosures

The HIPAA Privacy Rule requires you to have policies that protect and limit how you use and disclose PHI, but you aren't expected to guarantee the privacy of PHI against all risks. Sometimes, you can't reasonably prevent limited disclosures, even when you're following HIPAA requirements.

- For example, a hospital visitor may overhear a doctor's confidential conversation with a nurse or glimpse a patient's information on a sign-in sheet. These incidental disclosures aren't a HIPAA violation as long as you're following the required reasonable safeguards.

SECURITY RULE

The Security Rule includes security requirements to protect patients' ePHI confidentiality, integrity, and availability. The Security Rule requires you to:

- Develop reasonable and appropriate security policies
- Ensure the confidentiality, integrity, and availability of all ePHI you create, get, maintain, or transmit
- Identify and protect against threats to ePHI security or integrity
- Protect against impermissible uses or disclosures
- Analyze security risks in your environment and create appropriate solutions
- Review and modify security measures to continue protecting ePHI in a changing environment
- Ensure employee compliance

BREACH NOTIFICATION RULE

When you experience a PHI breach, the Breach Notification Rule requires you to notify affected patients, HHS, and, in some cases, the media. Generally, a breach is an unpermitted use or disclosure under the Privacy Rule that compromises the security or privacy of PHI. The unpermitted use or disclosure of PHI is a breach unless there's a low probability the PHI has been compromised, based on a risk assessment of:

- The nature and extent of the PHI involved, including types of identifiers and the likelihood of re-identification
- The unauthorized person who used the PHI or received the disclosed PHI
- Whether an individual acquired or viewed the PHI
- The extent to which you reduced the PHI risk

You must notify authorities of most breaches without reasonable delay and no later than 60 days after discovering the breach. Submit notifications of smaller breaches affecting fewer than 500 patients to HHS annually. The Breach Notification Rule also requires your business associates to notify you of breaches by the business associate.

PERMITTED USES AND DISCLOSURES

A covered entity is permitted, but not required, to use and disclose PHI without an individual's authorization, for the following purposes or in the following situations:

1. To provide the individual patient with their own PHI
2. For Treatment, Payment, and Health Care Operations
    - For continuity of care, reimbursement, or quality improvement audits or reviews
3. When the individual is given the opportunity to agree or object to the use or disclosure of their PHI (?)
4. Incident to an otherwise permitted use and disclosure
5. For Public Interest and Benefit Activities
    - Required by law (including statute, regulation, or court order)
    - Public health activities
    - Victims of abuse, neglect, or domestic violence
    - Health oversight activities
    - Judicial and administrative proceedings
    - Law enforcement purposes
        - Court orders, warrants, or subpoenas
        - To identify or locate a suspect, fugitive, material witness, or missing person
        - Victim or suspected victim of a crime
        - When a covered entity believes that PHI is evidence of a crime that occurred on premises
    - Decedents – disclose PHI to funeral directors, coroners, or medical examiners
    - Cadaveric organ, eye, or tissue donation
    - Research
    - Serious threat to health or safety
    - Essential government functions
    - Workers' Compensation
6. In a Limited Data Set for research, public health, or health care operations.

Covered entities may rely on professional ethics and best judgments in deciding which of these permissive uses and disclosures to make, and ensure minimum necessary standard disclosure of PHI.

ASSESSMENT

Ophthalmic practices have potential liability exposures due to HIPAA violations. These types of exposures include data security and privacy breaches as well as cyberattacks. The following are HIPAA-related recommendations for common inquiries:

- OMIC's *Professional Liability* policy under *Additional Benefits, Broad Regulatory Protection (BRP)* provides coverage for HIPAA Proceedings, which covers legal expenses and fines and penalties up to $100,000 for government actions alleging HIPAA privacy and security violations. The *Additional Benefit, e-MD™ Protection* provides coverage for Security and Privacy Liability, Regulatory Defense and Penalties, and Breach Response and Notification Costs. Click on the link to read the specifics on the BRP and e-MD™ Protections.
- When responding to social media reviews, be aware that acknowledging the reviewer as a patient can trigger an unauthorized HIPAA breach; review the recommended guidelines.

- Corresponding with patients via email and text can also result in HIPAA violations if the transmission is not secure or encrypted.

- Release of medical records guidance: HIPAA Authorizations and medical record requests and Q&A.

- HIPAA Journal: What is a HIPAA Violation and HIPAA Compliance Checklist?

RISK RECOMMENDATIONS

- Conduct HIPAA training with new staff and periodically with all staff
- Consider appointing a Privacy and Security Officer
- Develop policy and procedures for managing patient requests for access, corrections, and data transfer of PHI
- Conduct an audit to determine where PHI is created, received, stored, or transmitted, and how it is shared with Business Associates
- Ensure you have appropriate Business Associate Agreements in place
- Ensure electronic communication is secure and/or encrypted
- Identify risks and minimize the number of record sets in which PHI is maintained to simplify the management and protection of PHI
- Create measures to report data breaches

- Develop a plan for responding to an emergency that damages/breaches systems or physical locations where PHI is maintained
- Review state-specific laws and regulations concerning patient information security and privacy and monitor changes
- Become familiar with the *Additional Benefits* of your OMIC policy described above
-

RESOURCES

1. Medicare Learning Network. (2023). *HIPAA Basics for Providers: Privacy, Security, & Breach Notification Rules*. HIPAA Basics for Providers
2. Health and Human Services. (2017). *HIPAA for Professionals*. HIPAA for Professionals
3. HealthIT.gov. (2019). *Privacy, Security, and HIPAA*. Privacy, Security, and HIPAA
4. The HIPAA Journal. (2024). *HIPAA Compliance Checklist.* *HIPAA Compliance Checklist*

Need confidential risk management assistance?
OMIC-insured ophthalmologists, optometrists, and practices are invited to contact OMIC's Risk Management Department at (800) 562-6642, option 4, or at riskmanagement@omic.com.