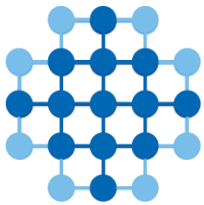


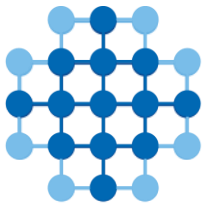
HIPAA Training



UB|MD
PHYSICIANS' GROUP

HIPAA Training Agenda

- What is HIPAA?
- HIPAA Enforcement
- Protected Health Information (PHI)
- Privacy Rule
- Patients' Rights
- Minimum Necessary
- Notice of Privacy Practice (NPP)
- Pediatric Patients
- Security Rule
- Three HIPAA Security Safeguards
- Breach Notification Rule
- Information Blocking
- Business Associates Agreement
- Cell Phone & Email Usage
- Important HIPAA Reminders
- Reporting HIPAA Violations
- HIPAA Case Examples



UB|MD

PHYSICIANS' GROUP

What is HIPAA?

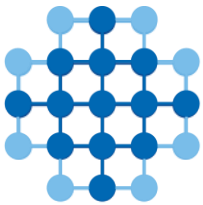
HIPAA stands for:

- ❖ Health
- ❖ Insurance
- ❖ Portability and
- ❖ Accountability
- ❖ Act

HIPAA is a broad Federal Law that establishes basic privacy protections to which all patients in the United States are entitled. It gives them the right to access their own health records, and to have their health information kept private and secure.

HIPAA establishes standards to safeguard the protected health information (PHI) that you hold if you are one of these covered entities or their business associate:

- Health plan
- Health care clearinghouse
- Health care provider/hospital/organization



UB|MD
PHYSICIANS' GROUP

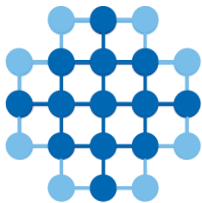
HIPAA Enforcement

The Office of Civil Rights (OCR) enforces HIPAA Rules.

OCR will watch and enforce the following:

- Unpermitted PHI use and disclosures.
- Use and disclosure of more than the **minimum necessary** PHI.
- Lack of PHI safeguards.
- Lack of Administrative, Technical, and Physical ePHI Safeguards.
- Lack of patients' access to their PHI.

❖ This is **not an exclusive list** to OCR enforcement actions.

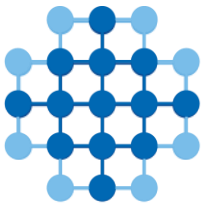


Protected Health Information (PHI)

Information is considered protected health information if you hold or transmit it in any form, including electronic, paper, or verbal.

PHI includes information regarding:

- Eighteen Common Identifiers
 - Can you recreate the patient information with 4 or fewer identifiers?
- The patient's past, present, and future physical or mental health condition.
- Medical records
 - Diagnosis codes, test results, doctor notes
- Documentation
 - Appointment scheduling notes
 - Prescription records
 - Health-related emails
- Billing/Payment information
 - Claims
 - Payment history
 - Health plan beneficiary numbers

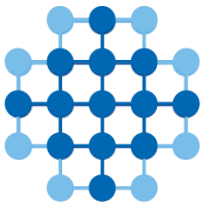


UB|MD

PHYSICIANS' GROUP

PHI: 18 Common Identifiers

- Name
- Address (all geographic subdivisions smaller than state, including street address, city county, and zip code)
- All elements (except years) of dates related to an individual (including birthdate, admission date, discharge date, date of death, and exact age if over 89)
- Telephone numbers
- Fax number
- Email address
- Social Security Number
- Medical record number
- Health plan beneficiary number
- Account number
- Certificate or license number
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Web URL
- Internet Protocol (IP) Address
- Finger or voice print
- Photographic image - Photographic images are not limited to images of the face.
- Any other characteristic that could uniquely identify the individual

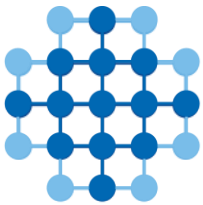


UB|MD
PHYSICIANS' GROUP

Primary Rules of HIPAA

HIPAA is built on three primary rules:

- **Privacy Rule**
Sets the standard for who can look at and receive patients' PHI.
- **Security Rule**
Outlines the safeguards that must be put in place by healthcare organizations to keep patients' digital data safe from hackers and unauthorized access.
- **Breach Notification Rule**
Mandates accountability if PHI is compromised in a data breach.



UB|MD

PHYSICIANS' GROUP

The Privacy Rule

The Privacy Rule protects patients' protected health information (PHI) and allows you to exchange information and coordinate your patient's care securely, and shifts control of health data back to the individual.

The Privacy Rule:

- Covers all forms of PHI, whether spoken, written on paper, or transmitted electronically.
- Dictates that healthcare providers and insurance companies can generally only share patient information for treatment, payment, and healthcare operations unless the patient gives them explicit written permission.



UB|MD

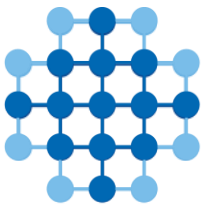
PHYSICIANS' GROUP

Patients' Rights

Patients have several different rights under the privacy rule, some of which are the following:

- Examine and receive a copy of their medical record, including an electronic copy of their medical records within 10 days in New York State.
- Request corrections to their medical records, and receive a response to the request. Provider must respond to such a request within 60 calendar days.
- Limit their plan's access to information about treatments they paid cash for.

NOTE: Under the Privacy Rule, you are allowed to report child abuse or neglect to the authorities.



UB|MD
PHYSICIANS' GROUP

Minimum Necessary

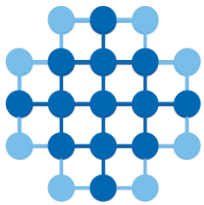
In HIPAA Privacy, the Minimum Necessary Rule is often referred to as the Golden Rule. This means sharing only the essential amount of PHI required to perform a specific task.

HIPAA requires healthcare workers to use or share only the minimum necessary information to perform their job duties.

Ask yourself these important questions when looking at private health information:

1. Do I need this information to perform my job and provide good patient care?
2. What is the least amount of information I need to perform my job?

If you find you do not have the access that you have, then let your supervisor immediately know.

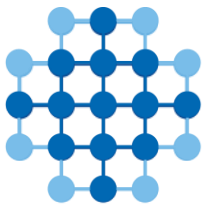


Minimum Necessary



“Minimum Necessary” Keys:

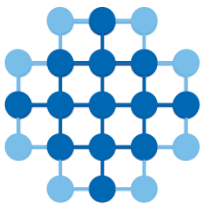
- **Limit Access:** Only employees who *need* the information to do their jobs should have access to it.
- **Limit Disclosure:** Share only the *minimum amount* of PHI required to achieve a specific purpose.
- **Exceptions:** This rule does *not* apply when sharing information with other providers for a patient’s treatment or when a patient requests their own records.



Notice of Privacy Practices

The Privacy Rule Requires that we notify patients about their privacy rights and how you use and share their information. This is called a **Notice of Privacy Practices**, and the patient must receive this at the time of their first appointment or prior to that appointment.

- The patient does not have to sign the Notice of Privacy Practices, also known as the “acknowledgment of receipt of the notice.”
- The provider must keep the NPP on file, either with the signed attestation or notation of the patient’s refusal to sign.
- Not signing the NPP does not give the provider rights to disclose privacy information. The patient is still protected under HIPAA.

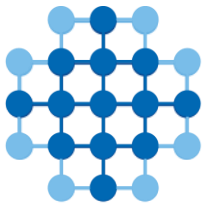


Pediatric Patients

Navigating the intersection of federal HIPAA regulations and New York State (NYS) laws for pediatric patients involves balancing parental rights with the growing privacy rights of the minor. In New York, the rules often lean toward protecting the minor's confidentiality as they approach adolescence.

Questions often arise regarding:

- Authorized signatories and personal representatives
- Identifications & documentation requirements
- Records release
- Custody and guardianship considerations



UB|MD

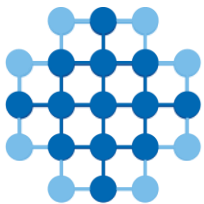
PHYSICIANS' GROUP

Pediatric Patients: Authorized Signatories & Personal Representatives

For most minors, the parent or legal guardian is the default representative and can sign for the release of records.

New York State Specifics:

- **Joint Custody:** Either parent can typically sign for records unless a court order explicitly says otherwise.
- **Sole Custody:** The custodial parent has decision-making authority, but the non-custodial parent still has a right to access records unless parental rights have been terminated, or a court order specifically prohibits access.
- **Foster Parents:** Generally **cannot** sign for the release of records. This authority usually remains with the local Department of Social Services (DSS) commissioner or the biological parent (if rights are intact).
- **Temporary Caregivers:** NYS allows a "Designation of Person in Parental Relationship" form, which permits a non-parent (like a grandparent) to consent to treatment and access records for up to six months.



UB|MD
PHYSICIANS' GROUP

Before giving PHI to anyone, always check for and carefully review waivers and/or court orders on file.

Pediatric Patients: Identification & Documentation Requirements

To obtain minors' records in NYS, providers **require** proper identification.

- **Requestor's Photo ID:** Valid state-issued driver's license, non-driver ID, or passport. **Always be sure to check ID!**
- **Proof of Relationship:**
 - **Minor's Birth Certificate:** Frequently required to prove the parent-child link if the parent is not already on file.
 - **Court Orders:** Documentation of legal guardianship, adoption papers, or specific custody agreements if there are restrictions on either parent.
- **Written Request:** Must have a completed and signed "Authorization for Release of Health Information Pursuant to HIPAA" (OCA Official Form No.: 960) to disclose PHI to third parties such as family members, attorneys, or insurers.

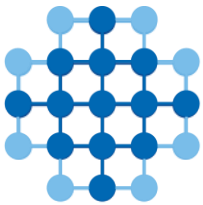
Before giving PHI to anyone, always check for and carefully review waivers and/or court orders on file.



Pediatric Patients: “12-Year-Old Rule” in New York

NYS Public Health Law contains a unique provision regarding minors and their records:

- **Notification:** If a parent/guardian requests the records of a minor **over the age of 12**, the provider **may notify** the minor of the request.
- **Right to Object:** If the minor objects to the disclosure, the provider has the discretion to **deny the parent's request** for access, provided the provider believes disclosure would be detrimental to the provider-patient relationship or the minor's care.



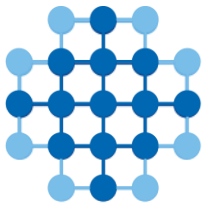
Pediatric Patients: Minor-Consented Services

In New York State, when a minor is legally allowed to consent to their own care in NYS, **they control the record**. Parents do not have an automatic right to see records related to:

- **Reproductive Health:** Pregnancy tests, prenatal care, and abortion.
- **Sexual Health:** STI/HIV testing and treatment (minors of any age can consent to STI care).
- **Substance Abuse:** Treatment for alcohol or drug dependency.
- **Mental Health:** Outpatient services (if the provider determines the minor is "mature enough" and involving parents would be detrimental).

Also in New York State, many patient portals cut off or limit parental access once the child hits 12 or 23 years of age to protect teen privacy.

Note on Waivers: For a parent to see these "sensitive" records, the minor must sign a specific waiver or authorization and specifically initial the sections for HIV, mental health, or substance abuse.



UB|MD

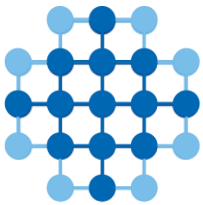
PHYSICIANS' GROUP

Security Rule

While the Privacy Rule covers *who* is allowed to see medical data, the Security Rule focuses on the *how* – the security measures needed to defend digital health data against breaches, accidents, and hackers.

The Security Rule is anchored by the security concept known as the CIA Triad - Confidentiality, Integrity, and Availability. In healthcare, it is sometimes referred to as the HIPAA Triad, and translates as follows:

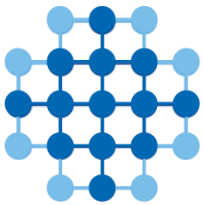
- **Confidentiality:** Restricting access to ePHI so only authorized people can see it.
 - *Example:* Using multi-factor authentication and data encryption so a lost laptop doesn't lead to exposed patient records.
- **Integrity:** Ensuring that patient data is accurate and has not been improperly altered.
 - *Example:* Keeping tracking systems (auditing) to see exactly who edited, or even viewed, a patient's chart and when.
- **Availability:** Making sure authorized users can get to the data when they need it.
 - *Example:* Having ironclad data backups and disaster recovery plans in place to providers can still treat patients during power outages or a ransomware attack.



Security Rule

The Security Rule includes security requirements to:

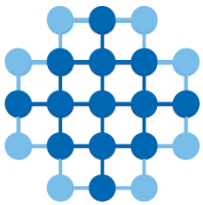
- Develop reasonable and appropriate security policies for your organization.
- Ensure Confidentiality, Integrity, and Availability of all ePHI you create, get, maintain, or transmit.
- Identify and protect against threats to ePHI security or integrity.
- Protect against impermissible uses or disclosures
- 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.**



Three HIPAA Security Safeguards

HIPAA security has many layers of protection, and within these layers of protection are certain safeguards that covered entities must comply with to reasonable standards. They are the following:

- **Administrative Safeguard:** This includes workforce training, risk analysis, management, HIPAA Information Security Officer, Incident Response Management, and Disaster Response Planning.
- **Physical Safeguard:** These are defined as “physical measures, policies, and procedures to protect a covered entity’s electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.” This would include:
 - Facility access controls
 - Workstation security (making sure computer monitors containing patient charts aren’t visible to the waiting room, or others who shouldn’t have access to them)
 - Mobile device security.
- **Technical Safeguard:** These are technology-based methods used to protect ePHI and control access to it. For example, Access controls, Audit Controls, Firewall Security, Data back up, and device and media Controls.



Breach Notification Rule

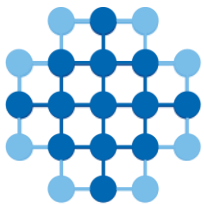
If you think you might have a breach, **IMMEDIATELY** call the Compliance Office and ask for assistance.

If a PHI breach is experienced, you must follow the Breach Notification Rule. The rule requires you to notify affected patients, HHS, and, in some cases, the media, depending on the number of affected individuals.

What is a breach?

Generally, a breach is an unpermitted use and 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 is a **LOW** probability the PHI has been compromised, based on a risk assessment of the following:

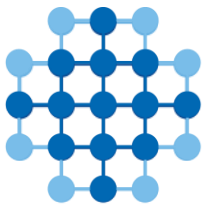
- The nature and extent of the PHI involved, including types of identifiers and the likelihood of re-identification.
- The unauthorized person who used the PHI or got the disclosed PHI.
- Whether an individual acquired or viewed the PHI.
- The extent to which you reduced the PHI risk.



Breach Notification Rule

HHS (Health and Human Services) Notification of Breach Information:

1. A Provider or Organization must notify authorities of most breaches without reasonable delay **and no later than 60 days after discovering the breach.**
2. Submitting notifications of smaller breaches affecting fewer than 500 patients to HHS can be done annually.
3. **Greater than 500 patients** by Covered Entities (CE) are required to provide notice to prominent media outlets serving the state jurisdiction. This will be in the form of a press release to appropriate media outlets serving the affected area. It must also be done in a timely manner and **within 60 days.**
4. The Breach Notification also requires Business Associates to notify you of breaches at or by the Business Associate.



UB|MD

PHYSICIANS' GROUP

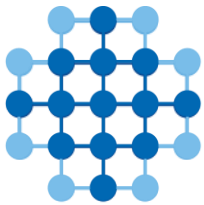
Further information can be found on the HHS site under the following link:

<https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html>

Information Blocking

Most clinical information is digitized, accessible, and shareable thanks to several technology and policy advances making interoperable, electronic health record systems widely available. In 2016, the 21st Century Cures Act (Cures Act) made sharing electronic health information the expected norm in health care by authorizing the Secretary of Health and Human Services (HHS) to identify "reasonable and necessary activities that do not constitute information blocking." The Office of National Coordinator for Health Information Technology (ONC) 2020 Cures Act Final Rule established information-blocking exceptions to implement the law.

Interfering with or blocking access, exchange, or use of electronic health information (EHI) except as required by law will prompt an investigation by HHS.

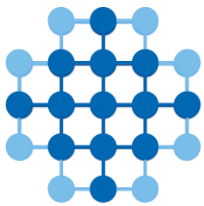


Business Associate Agreement

What is a HIPAA Business Associate Agreement (BAA)?

- Most often a BAA is a contract between a HIPAA-covered entity (CE) and a business or individual that performs certain function(s) or activities on behalf of, or provides a service to, the covered entity when the function, activity, or service involves the creation, receipt, maintenance or transmission of Protected Health Information (PHI).
- A Business Associate must follow the same stipulations for all HIPAA privacy and security regulations as the CE. However, depending on the agreement, they may have additional regulations, such as those with the FTC.
- Examples of organizations that typically have BAAs with healthcare providers:
 - ✓ Accountants, Lawyers, Collection Agencies, and Billing Companies

Having a Business Associates Agreement in place offers assurances that privacy and security standards are met.



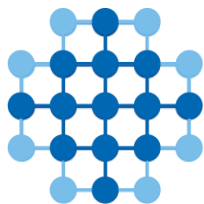
Using Cellphones

Reminder:

Keeping patient information or images on your private cell phone for UBMD is **NOT** allowed.

- You may be held personally liable for fines if the confidentiality of the patient is violated and breached.

Only secured text messaging is allowed with a secured text message that is encrypted and authorized by UBMD.



UB|MD

PHYSICIANS' GROUP

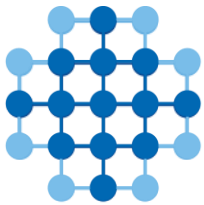
HIPAA and UBMD Email

UBMD Email Reminder:

DO:

ONLY SEND PATIENT INFORMATION
VIA SECURED FORMAT IN A ZIX
MESSAGE OR ANOTHER APPROVED
UBMD SECURED FORMAT

1. **Do NOT** include private health information for patients in your unencrypted emails.
2. **Do NOT** put patient information in the subject line of the email. Including:
 - Name/DOB
 - Medical Record Number
 - Account Number
3. **Do NOT** send images that can identify a patient by email.



UB|MD

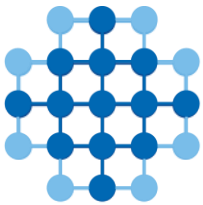
PHYSICIANS' GROUP

This Photo by Unknown Author is licensed under [CC BY-SA](#)



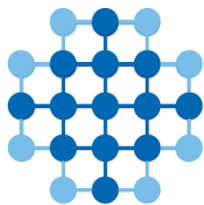
HIPAA Good Habits

- Establish STRONG passwords for your log-ins.
- Do not leave Post-it notes with the passwords viewable for easy access for others to see - secure them.
- **Do not share your passwords**; HIPAA is not a free streaming service.
- Control+ALT+Delete to lock your computer screen whenever you're away from your seat, even for a minute. This will prevent someone else from logging onto your system without a password.
- Be aware if someone remotes into your computer. Did you ask for technical assistance from OMC, for example?
- Be cautious of spam and phishing emails - you will get these!
- Be aware of suspicious emails or attachments - bad actors are very tricky and can make you act urgently to open your email and attachments!



Risky HIPAA Habits

- **Do not** search or look at your own medical records or for friends, family, co-workers, and VIP's health information. Speak to the Compliance Office for further questions on this topic.
- **Do not** post patient's private health information on social media.
- **Do not** text or email private health information UNLESS:
 - You need to Text/Email as it relates to your job function and treatment, payment, and operations (TPO). Make sure it is in a secured and encrypted platform.
 - Follow the Minimum Necessary Rule as it pertains to the access necessary to perform the needed functions of your job and patient care.
 - Patient requests transmittal of unencrypted PHI and we respond to that email.
- Avoid downloading malicious files and searching websites that are not secure.
- Not appropriately disposing of private health information. Make sure you use the correct and secured disposal bins.

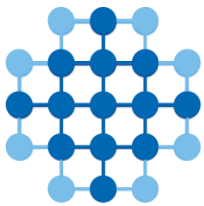


UB|MD

PHYSICIANS' GROUP

Risky HIPAA Habits - Continued

- Make sure you are speaking in low tones and discreetly about a patient's health information. Do not speak in public areas such as an elevator, restrooms, cafeterias, or hallways.
- Be aware of what information you are leaving on voicemails, whether it be on an answering machine or voicemail system such as on a cell phone. Leave the minimum information necessary.
 - HHS guidance is as follows: A covered entity (CE) might want to consider leaving only its name and number and other information necessary to confirm an appointment or ask the individual to call back. Do not leave details.
- **Do not** leave medical charts available and accessible to unauthorized personnel. Secure the information if you are not at your desk or workstation.
- **Do not** leave patient information on scanners or fax machines for extended periods of time. Make sure you check that periodically and secure the information to the appropriate intended source.



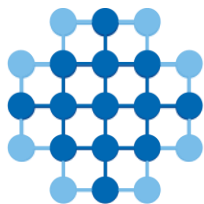
Risky HIPAA Habits - Continued

- **Do not** respond to online negative reviews regarding patient information or treatment. Instead, ask the reviewer to contact the office to discuss this further. If it is a positive review, thank them for their positive feedback and experience with UBMD.



When in doubt:

Please contact the
Compliance Office to ensure
HIPAA Privacy Compliance.



UB|MD

PHYSICIANS' GROUP

Reporting HIPAA Violations

As healthcare workers and UBMD employees, you are **obligated** to immediately report any **known or suspected** violations of HIPAA or any other misconduct, violations of law, acts of retaliation, or other wrongdoing.

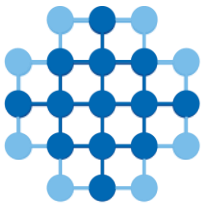
Reports may be made in any the following ways:

- Report directly to a practice plan supervisor.
- Report directly to the UBMD Chief Compliance Officer.
- Call the anonymous Compliance Hotline at 716.888.4752.
- Complete a Compliance Issue Reporting Form, which is available via our UBMD Compliance Office website.

<https://www.ubmd.com/about-ubmd/Compliance/Compliance-hotline-reporting.html>

A report of misconduct alone does not automatically lead to the discipline of the subject of the report. For this reason, employees are encouraged to contact the UBMD Compliance Office to discuss or report situations, even if the reporting individual is not certain that the situation in question rises to the level of noncompliance.

UBMD's non-retaliation policy will always be strictly adhered to.



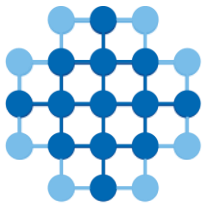
UBMD Compliance Hotline

UBMD COMPLIANCE HOTLINE: 716.888.4752

The Compliance Hotline is a non-traceable voicemail box, regularly monitored during business hours. When calling the Hotline, you may remain anonymous if you wish, but it is necessary that you provide all relevant information to the incident being reported:

- Practice Plan/Department;
- Date(s) & time(s) of incident(s);
- Detailed description of the incident or behavior in question;
- Name(s) of the person in question;
- Any other pertinent information.

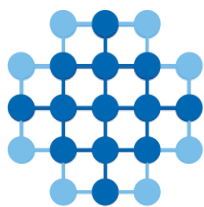
*Since the hotline is **not** monitored 24/7, if **there is an immediate threat to person or property involved**, please **DO NOT** leave a message. Contact your direct supervisor immediately!*



UB|MD
PHYSICIANS' GROUP

UBMD's non-retaliation policy will always be strictly adhered to.

HIPAA Case Examples



UB|MD
PHYSICIANS' GROUP

HIPAA Examples

Case 1:

You are reviewing a chart for coding and billing. You notice the patient is a Buffalo Bills player who has received services at a UBMD practice. You are excited to read about one of your favorite players. At lunch, you can't wait to tell your co-worker that you have the "scoop" on what is really happening with the player for next week's game.

Is this a HIPAA violation?

If this is a HIPAA violation, how is this a HIPAA violation?



Case Example #1 Breakdown

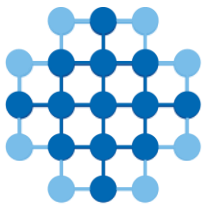
Is this a HIPAA Violation?

Yes, this is a HIPAA violation; disclosing patient information is a HIPAA violation without the purpose of treatment, payment, or operational means.

How is this a HIPAA violation?

The co-worker does not need any of this information about the celebrity sports player to perform their job. This was inappropriate. Under HIPAA, this is a privacy disclosure, and the patient's privacy was disclosed and violated.

Patients receiving medical care expect privacy, and they expect a level of privacy no matter who they are. They expect a level of interaction that will be respected, and their PHI will not be shared.



UB|MD

PHYSICIANS' GROUP

Case Example 2

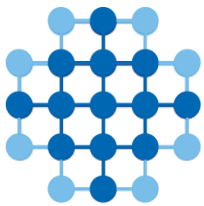
Case Example 2:

You work for a UBMD practice, and a patient has requested their medical records. They have placed a request for their personal health information. The patient has filled out, signed, and paid for the necessary documentation. The patient has been waiting over 30 days for the information.

Is this a HIPAA Violation?

Yes. This falls under Patient Information Blocking. Patients have a right to their medical records in a reasonable time. Denying patients their medical records because they cannot pay for the copy fee or overcharging them for the copy fee is a direct violation of HIPAA. Typically, in NYS, access to medical records is within 10 days of the request.

There are exceptions to this rule; for example, if the physician feels the information in the records may harm the patient or others.



UB|MD
PHYSICIANS' GROUP

Resources

Further Information can be found at the following sites :

<https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/Downloads/HIPAAPrivacyandSecurity.pdf>

<https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html>

<https://www.hhs.gov/hipaa/for-individuals/notice-privacy-practices/index.html>

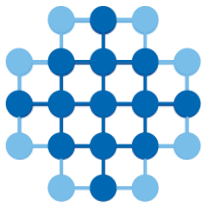
https://www.healthit.gov/sites/default/files/page2/2020-08/Health_Care_Provider_Definitions_v3.pdf

<https://oig.hhs.gov/reports-and-publications/featured-topics/information-blocking/>

<https://www.healthit.gov/topic/information-blocking>

<https://www.hipaajournal.com/hipaa-business-associate-agreement/>

<https://wnydocs.org/Release-of-Medical-Records#:~:text=Patient%20Access%20to%20Record&text=Although%20reasonable%20time%20is%20not,between%2010%20and%2014%20days>





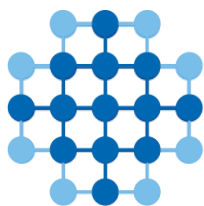
UBMD Compliance Office

Lawrence DiGiulio, Esq., Chief Compliance Officer

larryd@buffalo.edu

Suzanne Marasi, Compliance Administrator

smmarasi@buffalo.edu



UB|MD
PHYSICIANS' GROUP