



December 2024

Compliance Quarterly

From the Compliance Office...*The UBMD Compliance Hotline*

As 2024 comes to a close, we want to take this time to wish you and your families a joyous holiday season, and a happy, healthy New Year!! We look forward to continuing to work with you to grow the UBMD Compliance efforts in 2025!

Compliance Training Updates

Please note: All required training must be done by everyone personally. You should **not have coworkers summarize training programs or complete quizzes for you.*

2024 Mandatory Fraud, Waste & Abuse Training

The 2024 Mandatory Annual Fraud, Waste & Abuse Training was sent out via email on 10/23/24. All UBMD Practice Plan personnel are required to complete this training, including physicians, mid-levels, ancillary providers, registered nurses, licensed practical nurses, administrative and office staff, technicians, coders and others.

FWA training is a State and Federal requirement for ALL practice administration, providers & staff upon hire and annually thereafter. In addition, some 3rd party payers now require attestations of full staff completion.

The training will once again be posted to our website in the new year, making it easier to access for newly hired employees throughout the year.

2024 Mandatory Sexual Harassment Prevention Training

New York State requires **all persons** employed within the state to complete annual Sexual Harassment Prevention training. The hospital collaboration 2024 Mandatory Sexual Harassment Prevention Training was sent out on November 12th, with a completion deadline of December 20th. If you have not yet completed the training, we ask that you please do so at this time. The training can be accessed [here](#), and can be found on our UBMD Compliance website (<https://www.ubmd.com/about-ubmd/Compliance/Education-training.html>) under Education & Training. This training must also be completed by all new hires throughout the year.

Annual Cultural Competency Training

The NYS Department of Health requires that all providers complete cultural competency training on an annual basis. Most 3rd party payers require that **all** healthcare employees complete the training. Therefore, all UBMD personnel (providers and staff) should complete the training. At this time the only training they accept is NYS *Think Cultural Health* through the HHS.

The links and instructions for this training are on page 6 of this newsletter.

New Provider E/M & Documentation Training

Required for all newly hired providers. It also serves as a good refresher for not-so-new providers. This training is now available online by visiting the Education & Training page on the UBMD Compliance website. (<https://ubmd.com/about-ubmd/Compliance/Education-training.html>).

Inside This Issue

From the Compliance Office.....	1
Compliance Training Update ...	1
HIPAA: Common HIPAA Mistakes...	2
Improving Documentation.....	3
Copy & Paste Tip Sheet.....	4
Auditing & Monitoring in EMRs.....	5
Cultural Competency Link.....	6
Compliance Hotline.....	6
Compliance Quarterly Quiz.....	7

HELP US HELP YOU!!

We want you to be involved! Help us help you...if you have a question or topic you would like to see covered (general, specific or practice-focused) in a future edition of the *Compliance Quarterly*, please contact Sue Marasi at: smmarasi@buffalo.edu

HIPAA: Common HIPAA Mistakes and How to Prevent Them

Sue Marasi, CHC, CPCA, Compliance Administrator

According to the U.S. Department of Health & Human Services (HHS) website, as of July 31, 2024 (most recent update), the Office of Civil Rights (OCR) has received over 366,377 HIPAA complaints, and has initiated over 1,191 compliance reviews since the Privacy Rule's April 2003 compliance date. 99% (363,234) of those cases have been resolved. As of July 31, 2024 the OCR settled or imposed a civil monetary penalty in 147 cases resulting in a total dollar amount of \$143,728,972.

This illustrates how costly HIPAA violations can be due to monetary penalties. Include the possibility of jail time and negative publicity, and it becomes even more costly. Knowing how HIPAA breaches occur, and how to avoid them, is in everyone's best interest.

Most breaches are the result of HIPAA violations including:

- Failure to secure and encrypt data, which includes encryption on electronic devices, leaving paper documents out in the open, leaving computer screens open when you walk away.
- Theft of electronic devices.
- Employee misconduct, such as "snooping," which includes accessing patient records that aren't work-related (accessing records of family, VIPs, co-workers, etc.).
- Improper disposal of patient health information (PHI) and records, both paper and electronic devices containing sensitive information.
- Non-compliant partnership agreements.
- Lack of patient consent, denying patient access to their PHI, or exceeding the time limit for providing them access.

How can we prevent HIPAA violations? It takes all of us working together, having policies in place, following policies, and being aware of what you are doing at all times. This includes the following requirements:

- Conduct regular (at least annual) risk assessments to identify any potential risks or vulnerabilities to the confidentiality, integrity and availability of electronic PHI.
 - ⇒ Develop risk management plan to identify and address risks, and make improvements as necessary.
- Store PHI data securely when not in use.
 - ⇒ Never leave electronic devices unattended, out in the open, or in your vehicles.
 - ⇒ Log off computers every time you walk away from them.
- Ensure PHI is wiped from USB and drives, and shred paper documents containing PHI when they are no longer needed.
- Implement safeguards such as encryption on devices.
- Be sure to complete Business Associate Agreements with all vendors who are provided with or given access to PHI.
- Perform access and audit controls to prevent unauthorized access. The UBMD Compliance Plans requires that practice plans perform quarterly audits of EHRs as follows:
 - ⇒ Review records of VIPs to make sure records were only accessed by those who took part in the care and treatment of those patients.
 - ⇒ Review records of UBMD employees who are also practice plan patients to make sure records were only accessed by those who took part in the care and treatment of those patients.
 - ⇒ Perform random audits of up to five practice plan employees, and check one day from the previous quarter to make sure their access to records were appropriate.
 - ⇒ Any employee who performed inappropriate access found should face disciplinary action up to and including termination.
- Employee training
 - ⇒ HIPAA training is required upon hire and annually thereafter.
 - ⇒ Ensure all providers and staff understand the importance of:
 - ◆ Not sharing passwords
 - ◆ Authorized vs. unauthorized access to PHI
 - ◆ Securing devices at all times
 - ◆ Encryption of any devices used to access or share PHI
 - ◆ Proper disposal of records, electronic and paper
- If you are unsure if something is HIPAA-compliant, contact the Compliance Office.
- It is the responsibility and duty of all UBMD employees to immediately report any known or suspected HIPAA-related violations. You may do so by contacting the Compliance Office directly or via the confidential Compliance Hotline.



Improving Documentation Practices for 2025: A Fresh Start for Accuracy and Compliance

Sandy Setlock, CPC, CRC, CEMA, CHCO, Director of Audit & Education

As we close out the current calendar year and look forward to 2025, it's an ideal time to refresh and renew the habits we've developed over time—especially when it comes to documentation. Accurate documentation is crucial not only as a communication tool to convey essential patient information but also in supporting medical billing practices. To ensure we're setting ourselves up for success in the new year, let's review some key tips that will help enhance documentation standards and maintain compliance.

1. Be Cautious with "Copy and Paste" Features

While the "copy and paste" or "copy forward" features in Electronic Health Records (EHR) systems like Allscripts can improve efficiency, they also come with significant risks. These features often lead to what is known as "cloned documentation," which can raise concerns regarding both compliance and the integrity of patient records.

Each patient visit is unique, and the documentation for a specific date of service must accurately reflect the care provided during that encounter. Simply carrying forward text from a previous visit can result in documentation that does not accurately represent the current encounter, potentially leading to misrepresentation of the patient's concerns, treatment, and the plan of care on that day.

It's critical to remember that each patient is an individual, and their care should be documented in a way that reflects the work performed on the specific date of service. To maintain accurate documentation and ensure compliance, it is essential to avoid relying heavily on copied content from previous notes.

On page 4 of this newsletter you will find a tip sheet for Copy and Paste.

2. Utilizing Macros and Templates Carefully

Macros and templates can be incredibly helpful for streamlining patient documentation. However, they must be used carefully to ensure that each note is tailored to the specific patient and situation at hand. The temptation to use pre-existing templates without modification can lead to errors in documentation, such as upcoding or even incorrect entries that could be detrimental to patient care.

Misuse of templates or macros can result in documentation that doesn't accurately represent the patient encounter, leading to issues with billing or even legal consequences. Always ensure that any pre-filled content is reviewed, customized, and updated to align with the patient's current condition, treatment, and care plan.

By personalizing each note, even when using templates or macros, we can preserve both the accuracy of the patient record and the integrity of the medical documentation process.

3. Provider Queries: Be Mindful of Professional Communication

Electronic Health Record systems often include features that allow for messaging, tasking, and triage communications. While these tools are invaluable for coordinating patient care and communication between providers, it's important to remember that these messages are part of the patient's medical record.

In the event that a patient requests their records or legal entities require disclosure, these communications could be made available to external parties. As a result, any messages exchanged in the EHR should remain professional and focused on the care of the patient. Personal or casual messages, or communications intended for internal purposes (such as "friendly" interdepartmental messages), should be avoided in the medical record.

By keeping these messages relevant and professional, we ensure the patient's chart remains both compliant and respectful of privacy regulations.

Contact the Compliance Department for Support

If you have any questions about the topics outlined above or need further clarification, please don't hesitate to reach out to the Compliance Department. Our team is always available to provide guidance and elaborate on best practices for medical documentation.



The Coding Corner

Resources:

[MCD Documentation for Medical Professionals](#)

Tip Sheet on Copy and Paste

Sandy Setlock, CPC, CRC, CEMA, CHCO, Director of Audit & Education

Recent patient concerns have been raised nationally regarding copy-and-paste patient notes. The notes were generated from the provider's EHR. Unfortunately, we are seeing more of a trend of bringing forward a note or copying and pasting a note. In addition, we are seeing increased occurrences of "Note Bloat," which is too many pages of nonessential information, sometimes even concealing key parts of the patient's record.

In a recent scenario, a patient's documentation noted an open-heart surgery procedure. The patient never had this procedure; however, it was documented on a visit in detail and now had proceeded into several more notes to become "chart lore."

How did this happen? The provider copied a note from a chart they had opened and "pasted" or inserted the information into the wrong chart. A recent University of Pennsylvania Medical Center study found that from 2009-2018 electronic records became ubiquitous, and chart notes doubled in length.

How could this be avoided?

- Proofread/Validate your notes before signing off.
- Not having multiple patient charts open at the same time.
- Do not fill your notes with unnecessary copied details.
- Be alert to the details you are bringing forward into the patient's chart for accuracy.
- Remember, the narrative makes the encounter with the patient unique.

In 2016 CMS issued documentation integrity guidelines for the utilization of an EHR. The document stresses the importance of the integrity of the patient's medical record. Ensuring the integrity of the patient's medical record helps prevent fraud, waste, and abuse, confirms the continuity of patient care, and provides proper payment for services rendered.

In July 2021, the Joint Commission stated that the copy-and-paste function in a healthcare provider's clinical documentation improves efficiency; however, the copy-and-paste process can promote note bloat, internal inconsistencies, error propagation, and documentation in the wrong patient chart—all the mentioned potentially put patients at risk.

Utilizing an EHR has many incredible benefits, but the need to provide the mechanism and ensure the integrity of the patient's medical record is a priority. As a medical community, we must work together to ensure better patient processes and outcomes.



Resources:

<https://www.jointcommission.org/resources/news-and-multimedia/newsletters/newsletters/quick-safety/quick-safety--issue-10-preventing-copy-and-paste-errors-in-ehrs/preventing-copyandpaste-errors-in-ehrs/>
<https://www.statnews.com/2023/06/20/medical-records-errors-copy-paste/>



**More
Coding Corner**

General Compliance: Auditing & Monitoring in the UBMD EMRs

Sandy Setlock, CPC, CRC, CEMA, CHCO, Director of Audit & Education

The Importance of Auditing Users in Electronic Health Records (EHR)

In the age of digital healthcare, electronic health records (EHR) have become indispensable tools for managing patient information. However, as healthcare providers increasingly rely on EHR systems, ensuring the privacy and security of electronic protected health information (ePHI) becomes a critical responsibility. Among the various safeguards outlined by the Health Insurance Portability and Accountability Act (HIPAA), auditing user activities within EHR systems stands out as a key mechanism to maintain data integrity and security.

What is User Auditing in EHR?

User auditing involves monitoring and recording user activities within the EHR system such as Allscripts. This includes tracking which users access ePHI, what actions they perform, and when these activities occur. The goal is to ensure that access to sensitive health information is restricted to authorized individuals and that any improper actions are promptly identified and addressed.

Why is Auditing Users in EHR Important?

1. Enhancing Data Security

UBMD handles highly sensitive patient information. Unauthorized access or data breaches can have severe consequences, including compromising patient privacy and undermining trust. By auditing user activities, UBMD can detect and respond to suspicious behavior, such as unauthorized access attempts or unusual patterns of data usage.

2. Ensuring HIPAA Compliance

Under HIPAA, UBMD is required to implement audit controls as part of their technical safeguards for ePHI. These controls allow UBMD to record and examine activity in systems containing or using ePHI. Regular audits demonstrate compliance with regulatory requirements and provide documentation in case of an investigation or audit by authorities.

3. Promoting Accountability

Auditing user activities fosters a culture of accountability among staff. When users know their actions are monitored, they are more likely to adhere to security policies and avoid negligent or malicious behavior. This accountability helps protect the integrity of the EHR system and reduces the risk of data breaches.

4. Identifying and Mitigating Risks

User audits provide valuable insights into system vulnerabilities and potential threats. For instance, frequent access attempts by unauthorized users may indicate a security gap that needs immediate attention. By identifying such risks early, UBMD can implement corrective measures to safeguard patient data.

5. Supporting Incident Response

In the event of a data breach or security incident, user audit logs serve as a vital resource for forensic investigations. They help determine the scope of the breach, identify the individuals involved, and provide evidence for legal or regulatory proceedings.

Best Practices for Effective User Auditing

To maximize the effectiveness of user audits, UBMD has posted their Electronic Health Records Audits policy online within their Compliance Plan available for review at our Compliance Site and here at this link.

[UBMD Auditing Electronic Medical Records Policy](#)

Conclusion

Auditing user activities in EHR systems is not just a regulatory requirement, it is a cornerstone of effective data security and privacy management. By implementing robust audit controls, UBMD can enhance their ability to detect and respond to security threats, ensure compliance with HIPAA, and protect the trust that patients place in their care. In an era where data breaches are increasingly common, prioritizing user auditing is a proactive step toward safeguarding the future of healthcare and patient privacy.

If you have any further questions on this topic or how to implement the audit process, please reach out to the Compliance Office for further information.



“Alone we can do so little; together we can do so much.”

~ Helen Keller

Cultural Competency Training: Links and Instructions

As stated on page 1 of this newsletter, below are the links and instructions for required annual Cultural Competency Training.

PHYSICIANS & NURSE PRACTITIONERS: Please complete the course titled "A PHYSICIAN'S PRACTICAL GUIDE TO CULTURALLY COMPETENT CARE" and save your completion certificate in case you are asked to show proof of completion. Your Human Resources department or other practice representative may ask you to send certificates to them.

- Three courses are available to choose from (**you only have to complete one course per year**). Providers can alternate year-to-year between the various courses.
- If you have taken the program in its entirety and need to retake the program, request an email reset by emailing: contact@thinkculturalhealth.hhs.gov or calling: 833-485-1664.
- Please use this link for the physician/nurse practitioner course: <https://thinkculturalhealth.hhs.gov/education/physicians>

ADMINISTRATIVE & CLINICAL STAFF: Please complete the course titled "GUIDE TO PROVIDING EFFECTIVE COMMUNICATION AND LANGUAGE ASSISTANCE SERVICES".

- This course will **NOT** grant you a certificate of completion. Instead, you need to attest that you completed the training by going to <https://smbweb.med.buffalo.edu/ubmd/training.aspx> and selecting "2024 Think Cultural Health" from the Training Module dropdown menu. (The year will change annually, so it will soon change to "2025 Think Cultural Health.")
 - ⇒ Enter your UBIT Name if you have one. If not, leave blank.
 - ⇒ Enter your Last Name, First Name and select the practice plan that you are employed by.
 - ⇒ Click on "A" for Question 1. By doing so, you are attesting that you completed the training program.
- Please use this link for the administrative/clinical staff course: <https://thinkculturalhealth.hhs.gov/education/communication-guide>

Think Cultural Health can determine whether or not someone actually completed the program (should it come up during a state or federal investigation of a practice plan in the future), so it is strongly advised that no one sign the Attestation of Completion without actually doing the training.

UBMD Compliance Office Website:

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

CONTACT US:

77 Goodell St., Suite 310
Buffalo, NY 14203

Fax: 716.849.5620

Lawrence C. DiGiulio, Esq.
Chief Compliance Officer
716.888.4705
larryd@buffalo.edu

Suzanne Marasi, CHC, CPC-A
Compliance Administrator
716.888.4708
smmarasi@buffalo.edu

Sandra Setlock, CPC, CRC, CEMA, CHCO
Director of Audit & Education
716.888.4702
sandrased@buffalo.edu



COMPLIANCE HOTLINE

UBMD COMPLIANCE HOTLINE: 716.888.4752

CONFIDENTIAL!

Report known or suspected fraud/abuse, HIPAA concerns, or
other potential problems.

Ask questions or request guidance | Provide relevant information
Remain anonymous if you wish | Non-retaliation policy will be adhered to

CLICK HERE FOR PRINTABLE FLIER: [Hotline Flier](#)

(This is a voice mail box monitored during working hours. If there is an immediate threat to person or property, do not leave message; contact direct supervisor immediately!)

Compliance Quarterly Quiz

To submit your quiz answers, please click link below:

[2024 December Compliance Newsletter Quiz](#)

1. Which of the following are required to help to prevent HIPAA violations? ?
 - A. Storing PHI data securely when not in use.
 - B. Completing Business Associate Agreements with all vendors provided with or given access to PHI.
 - C. Performing quarterly access audits of EHR records.
 - D. All of the above

2. Which of the following is not a true statement regarding accurate documentation?
 - A. Any messages exchanged in the EHR messaging, tasking, and triage communications should remain professional and focused on the care of the patient, and shouldn't include messages intended only for internal use.
 - B. Each patient visit is unique, and the documentation for a specific date of service must accurately reflect the care provided during that encounter. Simply carrying forward text from a previous visit can result in documentation that does not accurately represent the current encounter, potentially leading to misrepresentation of the patient's concerns, treatment, and the plan of care on that day.
 - C. There is no risk in using the copy and paste or copy forward feature in the EHR.
 - D. Misuse of macros and templates can result in documentation that doesn't accurately represent the patient encounter, leading to issues with billing or even legal consequences.

3. Although the copy-and-paste function in a healthcare provider's clinical documentation improves efficiency, the copy-and-paste process can promote note bloat, internal inconsistencies, error propagation, and documentation in the wrong patient chart.
 - A. True
 - B. False

4. The goal of user auditing in the EHR system is to ensure that access to sensitive health information is restricted to authorized individuals and that any improper actions are promptly identified and addressed.
 - A. True
 - B. False

5. Auditing users in the EHR is important for what reasons?
 - A. Ensuring HIPAA Compliance and enhancing data security
 - B. Identifying and mitigating risks, promoting accountability, and supporting incident response
 - C. Both A and B are correct
 - D. None of the above