



3rd Quarter 2025

Compliance Quarterly

From the Compliance Office...

We hope everyone is enjoying Summer! We know everyone is busy, and training can seem overwhelming as we try to find a work/home life balance. However, as a reminder, training is important to ensure that all staff understand and adhere to the laws, regulations, and ethical standards in healthcare. Training helps prevent fraud, protect patient privacy, and promote safe, high-quality care. Importantly, it is also a legal requirement under both state and federal regulations, including HIPAA and other healthcare-specific laws. Failure to complete compliance training can result in serious legal consequences, financial penalties, and harm to UBMD's reputation. We ask that you please be sure to pay attention to the training updates provided in each newsletter.

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.*

HIPAA Training - Please use this updated training program going forward!

Earlier this year, we updated our HIPAA training program, which is now available on our UBMD Compliance Office website (<https://ubmd.com/about-ubmd/Compliance/Education-training.html>). **This is the program newly hired UBMD employees should be directed to complete going forward. The old program should not be distributed any longer.**

Although annual training is covered via completion of newsletter quizzes, and distribution of other alerts or notices we may send out throughout the year, this training program is a good refresher for existing employees as well.

2025 Mandatory Fraud, Waste & Abuse Training

2025 Mandatory Annual Fraud, Waste & Abuse Training was sent out on July 10th. If you haven't yet completed it, please go to the UBMD Compliance Office website and do so at this time. 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.

2025 Mandatory Sexual Harassment Prevention Training

NYS requires **all persons** employed within the state to complete annual Sexual Harassment Prevention training upon hire and annually thereafter. The hospital collaboration 2025 Mandatory Sexual Harassment Prevention Training will be sent out in October or November, and will have a completion deadline of mid-late December. Until then, the 2024 training program remains available for new employees and for existing employees who have not yet completed it. The training can be accessed [here](#), and can be found on our UBMD Compliance website under Education & Training.

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.

Annual Cultural Competency Training

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.



Inside This Issue

From the Compliance Office.....	1
Compliance Training Update	1
Critical Role of Documentation.....	2
HIPAA: Patient Right of Access.....	3
Different Types of Phishing Attacks..	4
2025 OIG Work Plan Highlights.....	5
Cultural Competency Link.....	6
Compliance Hotline.....	6
Compliance Quarterly Quiz.....	7

HELP US HELP YOU!!

We want you to be involved! 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

The Critical Role of Medical Documentation: A Case Study in Risk Management

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

Why Documentation Matters

Accurate and thorough medical documentation is a cornerstone of quality patient care and healthcare operations. It serves multiple essential functions, including:

- **Care Coordination:** Facilitates continuity and coordination of care among healthcare providers.
- **Professional Communication:** Ensures clear communication between multidisciplinary teams.
- **Billing and Reimbursement:** Supports claims for services rendered and ensures appropriate reimbursement.
- **Regulatory Compliance:** Demonstrates adherence to accreditation, licensure, and regulatory standards.

However, one of the most critical - yet often overlooked - reasons for meticulous documentation is **medical-legal protection**. Proper documentation can prevent litigation or serve as a strong defense in the event of a malpractice claim. Conversely, poor documentation can undermine even the most defensible case.

Case in Point: A Documentation Breakdown

Consider the following real-world malpractice claim involving a podiatric physician. The case illustrates how documentation errors can significantly hinder legal defense.

A 50-year-old female patient presented with a painful bunion. The podiatrist scheduled a modified McBride bunionectomy with metatarsal osteotomy and screw fixation. Postoperatively, the patient experienced pain and swelling, which she attributed to walking without crutches, contrary to medical advice.

At a one-month follow-up, X-rays revealed lipping on the metatarsal head and a backing-out screw. The podiatrist attributed these findings to overuse and performed a second surgery to remove the screw and revise the bunionectomy. Despite continued non-compliance, the patient was provided with a CAM walker and monitored over four visits. At the final visit, the podiatrist noted improvement and advised continued use of the walker. The patient did not return but instead sought care from an orthopedic surgeon, who diagnosed a "pin track infection." She later underwent a joint fusion and pain management procedures.

The patient filed a lawsuit alleging:

- Failure to attempt conservative treatment before surgery.
- Improper surgical technique.
- Failure to diagnose and treat an infection.
- Failure to refer to an infectious disease specialist.

Documentation Deficiencies Identified

Upon review, the defense team uncovered several critical documentation issues:

- **Inconsistent Laterality:** Initial records referenced the left foot, while the patient's complaint involved the right. This inconsistency persisted in subsequent notes.
- **Template Overuse:** The podiatrist admitted to using unmodified template language, resulting in inaccurate and vague entries.
- **Inadequate Operative Report:** Although the correct foot was noted, the report lacked detail about the procedure performed.
- **Antibiotic Use Unexplained:** Keflex and later Clindamycin were prescribed without documented rationale or clinical justification. No prescription records or sample logs were included.

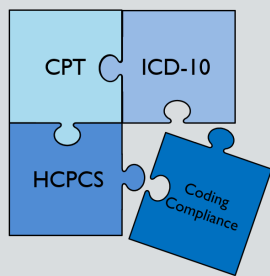
These documentation gaps made it impossible to determine whether an infection was present at the time of the second surgery or why antibiotics were prescribed. The podiatrist could not recall his clinical reasoning, and the records failed to support his decisions.

Outcome

Due to the weak documentation, the case could not be robustly defended and was ultimately resolved by payment of a settlement.

Conclusion

This case underscores the importance of accurate, individualized, and comprehensive documentation. Providers must avoid over-reliance on templates, copy/paste, and bring forward documentation to ensure that every entry reflects the specific clinical scenario. In the event of litigation, the medical record becomes the primary evidence of care provided. As this case illustrates, poor documentation can turn a defensible case into a liability.



The Coding Corner

HIPAA: Patient Right to Access

Sue Marasi, CHC, CPCA, Compliance Administrator

As healthcare workers, we play a vital role in ensuring patients can access their health records, which is a right guaranteed under **HIPAA**. Recent enforcement actions by the Office of Inspector General (OIG) and Office of the Medicaid Inspector General (OMIG) have made it clear that **timely and complete access to medical records is a compliance priority**.

What Is the HIPAA Right of Access?

Under the HIPAA Privacy Rule, patients have the legal right to inspect and obtain a copy of their protected health information (PHI) maintained by a covered entity. This includes medical and billing records in any format—electronic or paper.

Key requirements:

- It is important to know that **New York State law requires providers to grant patient access to their health records for inspection within 10 days of a written request, or copies within a reasonable timeframe, typically 15 days for copies**. This right is guaranteed by [New York's Public Health Law 18](#).
- Providers must reasonably verify the identity of the requestor.
- Fees must be reasonable and cost-based (e.g., labor for copying, supplies, postage). NYS allows a fee not exceeding providers incurred costs, with a maximum charge of \$.75 per page plus postage for paper copies.
- In NYS the maximum fee for electronic copies (CD, DVD, other electronic means) the lesser of \$.75 per page or \$100 total.
- For special records, such as x-rays, MRIs, etc., providers can charge the actual reproduction cost instead of a per-page fee.
- A patient cannot be denied a copy solely because they cannot afford to pay.

OMIG and OIG Enforcement Focus:

Both agencies have recently stepped up enforcement efforts, emphasizing:

1. **Timeliness of Responses**
Delayed access is the most common violation. Numerous fines have been issued - some exceeding \$100,000 - for providers failing to respond within 15 days.
2. **Accessibility for Vulnerable Populations**
OMIG has focused on ensuring that Medicaid recipients and individuals with disabilities or language barriers are not denied access due to administrative obstacles.
3. **Training and Documentation**
Healthcare workers must be trained to recognize and properly respond to access requests. Documentation of requests, responses, and identity verification is essential for compliance.
4. **Reasonable Fees**
Charging excessive fees or unnecessary costs can be a violation. Providers must review their policies to ensure fees align with HIPAA guidelines.

Best Practices for Healthcare Workers:

- **Know the policy:** Familiarize yourself with your organization's HIPAA access procedures.
- **Respond quickly:** Log and act on requests as soon as they are received.
- **Be patient-centered:** Help patients understand their rights and assist them in making requests.
- **Avoid unnecessary hurdles:** Don't require in-person visits or notarized requests unless legally required.

Compliance with the HIPAA Right of Access is not just a legal requirement, it's an essential part of delivering patient-centered care. By staying informed and responsive, healthcare workers can protect patients' rights and avoid enforcement actions.



Do You Know the Different Types of Phishing Attacks?

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

In this cyber threat environment, we now find ourselves in a swimming hole that keeps getting bigger and deeper, full of danger!

A brief time ago it was only just a few different types of phishing scams that were discussed, now there are at least 19 different type of phishing scams you should have some knowledge of. This article will list a few of these for your review and reference that remain at the top of the food chain for hackers.

Phishing involves a hacker (a.k.a. attacker-threat actor) trying to trick someone into providing sensitive account information. No account is safe from this type of hack. EVERYONE is a potential target. This means not only are your professional accounts here at UBMD at risk but also your personal accounts. The hackers (attackers) are trying to take advantage of you and get you to act. They will press upon you to act urgently or try to trick and entice you. They will make you think you are on a safe site when really it is a “fake or copied site.” When this happens multiple chain events can happen, malicious malware can be installed, your security to your accounts is breached and the UBMD securities and the practice plan you work with is now in jeopardy, your identity may be stolen, and your financial accounts may be compromised.

A new fishing vector has also now evolved with AI; the strategy and technology are evolving at a rapid pace. Vigilance is more important than ever!

Knowing the different types of Phishing attempts gives you the advantage and knowledge to protect yourself and UBMD. Here are some Top **Phishing Attacks for your knowledge**. Provided are a few examples along the way.

1. **Email Phishing:** In an email phishing scam, the attacker sends an email that looks authentic and legitimate. It is designed to trick the recipient into entering information for you to reply to or on a site that the hacker can use to steal or sell your data.

Example: Hackers used a LinkedIn profile to grab contact information from an employee at Sony Pictures and targeted them with an email phishing campaign. They got away with over 100 terabytes of data.

2. **Spear Phishing** involves targeting specific individuals in an organization to try to steal their login credentials. The attacker gathers information about the person before starting the attack, such as their name, position, and contact details. The “Spear” usually targets high profile individuals.

Example: An attacker tried to target an employee in Maintenance for a proposal for landscaping to be done for the company’s facility using spear phishing, The attacker claimed that the victim needed to sign new invoices that came into the Finance Dept for their work. To review the invoice, you would need to click on the hyperlink provided by inputting your username and password.

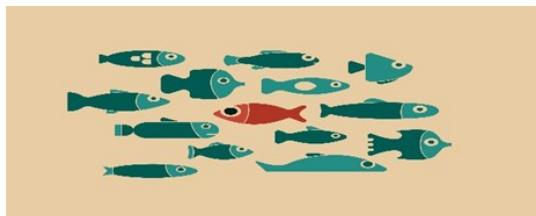
3. **Whaling:** A whaling attack is phishing attack that targets senior executives. These individuals often have deep access to sensitive areas of the network; a successful whale attack can result in valuable information being comprised from an entity.

Example: The CFO for a healthcare entity was the target of a Whale Attack; this attack led a group of employees to a “fake” connection using a fraudulent Zoom connection using the entity’s logos. After following the link, they had malware installed on their system. **(Example Scenario)**

4. **Vishing:** Is short for “voice phishing” is when someone uses the phone to try to steal information. The attacker may pretend to be a trusted friend or relative.

5. **Smishing:** Is a form of phishing that is sent from a text message or SMS message.

Example: Recently, there have been text messages stating they are from the NYS DMV stating if you do not click on the link, you will be fined, arrested, and lose your license. **(This is an actual text smishing currently)**



General Compliance

*If it looks
phishy,
it probably
is!*

Resources:

[Types-of-phishing-attacks](#)

cisa.gov/sites/default/files/2023-02/phishing-infographic-508c.pdf

6. **Website spoofing:** In this Phishing attempt, the hacker creates a website spoof that looks legitimate. When you log into your website account the hacker now has your credentials such as username and password. There are users out there that will use the same username and password over and over again, now the hacker can go into multiple accounts and have access to your confidential information.

Example: Hackers made a fake Amazon website; the Amazon users log in and put their username and password along with credit card information. The site looked nearly identical to the Amazon website. Now, hackers have access to important information about the user.

7. **Pharming:** In a Pharming attack, the victim gets malicious code installed on their computer. This code then sends the victim to a fake website designed to gather their login in credentials.

8. **HTTPS Phishing:** An HTTPS phishing attack is carried out by sending the victim an email with a link to a fake website. The site may then be used to fool the person into entering their confidential information.

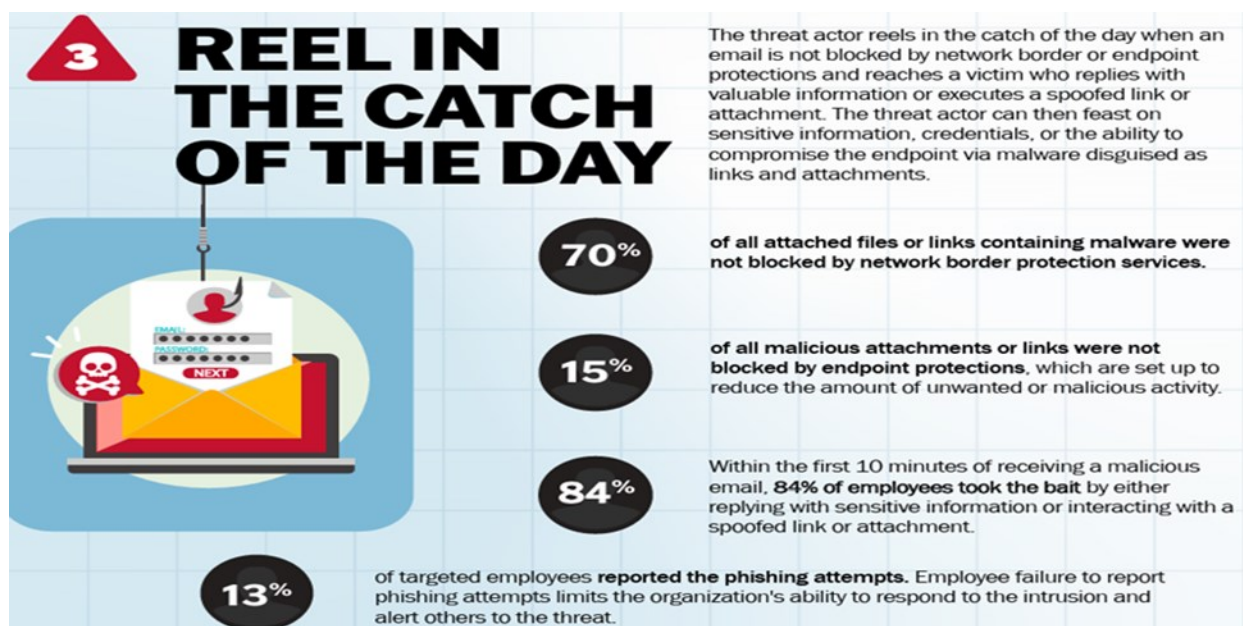
Example: A Hacker Group named Scarlet Widow, searched for employees' profile and emails at a company. Then then targeted the employees with HTTPS phishing sending them emails with hyperlinks to their "created website." Lesson here, do not click on a link you cannot verify or that is unknown.

9. **Social Media Phishing:** Attackers use social media platforms to impersonate legitimate organizations or individuals and trick users into providing information or clicking on malicious links.

Example: This can happen via LinkedIn, Facebook, X or Instagram. Accounts are copied and set up to entice other uses to engage. They will copy profiles and create a new account with the information they hacked from the legitimate profile and start to trick new users into providing information to them. **This is very dangerous professionally and personally. They will use AI to generate voice, and image to create a whole new profile.**

10. **Fake Apps:** Attackers create fake Apps for mobile applications that mimic legitimate apps and trick users into downloading them and providing confidential information. They can also be embedded with malicious malware to infect your devices once downloaded. **This is also happening with QR codes.**

In a recent CISA (Cybersecurity & Infrastructure Security Agency) assessment for the federal government to assess their vulnerability and expose the risk of compromise the following graph was published. 84% of employees took some interaction with the spoof link or attachment. That is alarming!



It is highly likely that in your professional or personal life you will encounter a form of phishing. Be alert, think and do not react. Act with logic and thought in this extremely fast paced life we all live.

If you have any questions, please contact the Compliance Department and the Office of Medical Computing (OMC).

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:

[2025 3rd Quarter Compliance Newsletter Quiz](#)

1. Documentation serves multiple essential functions in healthcare operating including which of the following?
 - A. Care coordination and professional communication
 - B. Billing and reimbursement
 - C. Regulatory and meaningful use compliance
 - D. All of the above
2. New York State law requires providers grant patient access to their health records for inspection within 10 days of a written request, or provide copies within a reasonable timeframe, typically 15 days for copies.
 - A. True
 - B. False
3. OMIG and OIG have stepped up patient access enforcement efforts, emphasizing which of the following?
 - A. Timeliness of responses and training and documentation
 - B. Accessibility for vulnerable populations and reasonable fees
 - C. Both A and B
 - D. Neither A nor B
4. All of the following are types of Phishing cyber threats except:
 - A. Spear Phishing
 - B. Ice Phishing
 - C. Whaling
 - D. Smishing
5. In a recent CISA (Cybersecurity & Infrastructure Security Agency) assessment for the federal government to assess their vulnerability and expose the risk of compromise, what percentage of employees took the phishing bait by either replying with sensitive information or interacting with a spoofed link or attachment.
 - A. 12%
 - B. 56%
 - C. 84%
 - D. 91%