2020 2nd Quarter
Volume 14, Issue 2

Compliance Quarterly

From the Compliance Office…

Coming up…

Our next newsletter (2020 3rd Quarter) will be the Annual Mandatory Fraud, Waste & Abuse Training. All UBMD personnel are required to complete this training.

Newsletter Topics

In the *Compliance Quarterly,* we focus on currently relevant Compliance & HIPAA topics, regulatory updates, and helpful tips. If anyone has a topic you would like to see covered, general or practice-focused, in a future edition of *Compliance Quarterly,* please contact Sue Marasi (smmarasi@buffalo.edu).

Compliance Training Update

New Provider E/M & Documentation Training

This is also a good refresher for the not-so-new providers! To be setup for this online training session, please contact Bev Welshans at welshans@buffalo.edu or 888-4702.

Lunch-n-Learn

Sessions are usually held once a month. Bring your lunch, and join us as we cover a variety of important topics related to coding and compliance!

AAPC & AHIMA CEUs are often available for the sessions. All are welcome to attend.

If you would like to be added to the session contact list, please contact Bev as noted to the right.

Please Note: Due to the COVID epidemic, Lunch-n-Learn sessions are currently on hold, but will be rescheduled once a new methodology for the training can be developed. At that time, an email will be sent to those on the contact list.

Inside this issue

Training Questions

If you have questions on any training, please contact Bev Welshans by telephone: 888-4702 or e-mail: welshans@buffalo.edu

HIPAA in the Time of COVID

By: Lawrence C. DiGiulio, Chief Compliance Officer

It is both comforting and frightening that, while the world has changed in the last several months, HIPAA remains inviolate in its refusal to adapt to the virus' whims. The HHS Office of Civil Rights (OCR) continues to prosecute actions against covered entities for violating HIPAA regulations.

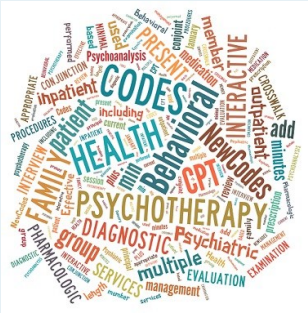
On July 27, 2020, OCR publicized its settlement with Lifespan Health Systems, a not for profit health system in Rhode Island, where Lifespan was fined $1,040,000 and required it to implement a corrective action plan as the result of a stolen laptop. OCR's director, Roger Severino, noted that "Laptops, cellphones, and other mobile devices are stolen every day, that's the hard reality. Covered entities can best protect their patients' data by encrypting mobile devices to thwart identity thieves." This quote makes clear that nefarious actions of third parties are not a defense to a HIPAA breach.

The fact that laptops and phones are regularly stolen is not a surprise to anybody. This fact led to a pair of UBMD policies. The first is that no Protected Health Information (PHI) may be stored on laptops or phones. Any PHI must be stored on our servers which are protected from accidental disclosures. The second is that all new laptops must be encrypted in case stray PHI finds its way onto a hard drive. There are still older laptops without encryption software installed on them. There are encryption products that can be installed in these older laptops and that step is recommended.

Not addressed in this most recent fine is the use of phones or laptops to send unencrypted PHI in text messages or email. The unencrypted electronic distribution of PHI is prohibited. Our hospital partners have encryption technology in place if electronic PHI transmission is required. Some practices have invested in such technology. If the phone or laptop is stolen, and the PHI is not encrypted at rest (when it is not being transmitted but when it is resident on the device) then it is still a breach and must be reported to OCR, who will then investigate the matter and that practice's HIPAA compliance. The easy way to avoid that unpleasant and potentially expensive encounter with federal government is to follow all HIPAA policies.

One HIPAA change caused by COVID is the temporary relaxation of HIPAA as it applies to telehealth. The rules were relaxed only to the extent non-encrypted electronic systems could be used for telehealth visits. This allowed practices to use ZOOM, Webex, Teams and other non-HIPAA compliant services to see and hear patients and provide medical services. This rule suspension lasts only as long as the Federal Government continues to declare the COVID Public Health Emergency. This declaration was just extended on July 24, 2020 for another ninety days.

We can never warn you enough about the danger of clicking links in emails that you do not know are real. There is a plethora of bad actors looking to phish your information to access our systems. If you think you have clicked on a link that was not related to work or that asked you for any personal information or your sign-on credentials, please call a member of the compliance team immediately. Also, contact our compliance team if you have any questions about HIPAA or any other issue.



Changes Are Coming to E/M Codes in 2021

By: Beverly Welshans, CHC, CPMA, CPC, COC, CPCI, CCSP
Director of Audit & Education

The Coding Corner

January 1, 2021 will usher in the most significant changes to Evaluation and Management (E/M) services we have ever seen. Regulatory changes have not always meant improvements. These changes, for the most part, are an improvement, making medical record keeping less arduous for providers while providing compensation for all the time clinicians devote to an outpatient encounter.

Over the next several months, I plan to share information with you in preparation for the change implementation date; first an overview, then more detailed information, key component by key component.

Overview of 2021 Changes:

These changes relate only to new and established outpatient visits, codes 99202-99215:

- Medicare adopted CPT E/M changes for 2021.
- Medicare rescinded the plan for bundled payment for three levels of codes.
- New and established patient visits can be based on time or medical decision making (MDM).
- New guidelines for using time for 99202-99215, new definitions in MDM.
- Code 99201 will be deleted.
- There will be no required level of history or exam for visits 99202-99215.
- Time will be defined as total time spent, including non-face-to-face work done on that day.
- Time no longer has to meet 50% rule nor be dominated by counseling.
- Visits will have a range for time; for example, 99213 will be 20-29 minutes, 99214 will be 30-39 minutes.
- The MDM calculation will be similar to, but no identical to, the current MDM calculation.

A closer look at *Time:*

Total time on the date of the encounter (office or other outpatient services [99202-99205, 99212-99215]):

For coding purposes, time for these services is the total time on the date of the encounter.

- It includes both the face-to-face and non-face-to-face time personally spent by the physician and/or other qualified health care professional(s) on the day of the encounter (includes time in activities that require the physician or other qualified health care professional).
- It does not include time in activities normally performed by clinic staff.

Physician/other qualified health care professional time includes the following activities, when performed:

- Preparing to see the patient (eg: review of tests);
- Obtaining and/or reviewing separately obtained history;
- Performing a medically appropriate examination and/or evaluation;
- Counseling and educating the patient/family/caregiver;
- Ordering medications, tests, or procedures;
- Referring and communicating with other health care professionals (when not separately reported;
- Documenting clinical information in the electronic or other health record;
- Independently interpreting results (not separately reported) and communicating results to the patient/family/caregiver;
- Care coordination (not separately reported).

All other E/M services that are defined by the three key components will continue to use the 1995 and/or 1997 Documentation Guidelines. Therefore, clinicians will have one set of rules for outpatient services and another for inpatient services.

Please feel free to contact Bev with any questions: welshans@buffalo.edu 888-4702

NEXT ISSUE

In our next issues, I will address the specifics of History, Exam and Medical Decision Making.

General Compliance: Several HHS OCR Communications & Alerts

By: Sue Marasi, CHC, CPCA, Compliance Administrator

The Health & Human Services Office for Civil Rights (HHS OCR) has put out several communications recently which remind us that, through the instability of the COVID pandemic, we all need to be even more aware of potential scams and fraud as we go through our workdays. The following are brief synopses of the communications sent.

Individual Posing as OCR Investigator

The OCR states that it has come to their attention that an individual posing as an OCR Investigator has contacted HIPAA covered entities in an attempt to obtain protected health information (PHI). The individual identifies themselves on the telephone as an OCR investigator, but does not provide an OCR complaint transaction or any other verifiable information relating to an OCR investigation.

Should you receive such a phone call, it is important that you verify someone is an OCR investigator by asking for the investigator's email address, which will end in @hhs.gov, and by asking for a confirming email from the investigator's hhs.gov email address. Should you have any questions or concerns regarding this alert, contact the UBMD Compliance Office.

∞∞∞∞∞∞∞∞∞∞

Guidance on Covered Health Care Providers and Restrictions on Media Access to PHI about Individuals in Their Facilities

The OCR issued additional guidance reminding providers that the HIPAA Privacy Rule does not permit them to give media and film crews access to facilities where patients' PHI will be accessible without the patients' prior authorization.

The guidance explains that even during the current Covid-19 public health emergency, covered health care providers are still required to obtain a valid HIPAA authorization for each patient whose PHI will be accessible to the media **before** the media is given access to that PHI. The guidance clarifies that masking or obscuring patients' faces or identifying information before broadcasting a recording of a patient is not sufficient, as a valid HIPAA authorization is still required **before** giving the media such access.

The guidance also describes reasonable safeguards that should be used to protect the privacy of patients whenever the media is granted access to facilities, which can include installing computer monitor privacy screens to prevent the film crew from viewing PHI on computers, and setting up opaque barriers to block the film crew's access to the PHI of patients who did not sign and authorization.

The guidance may be found at:
https://www.hhs.gov/sites/default/files/guidance-on-media-and-film-crews-access-to-phi.pdf

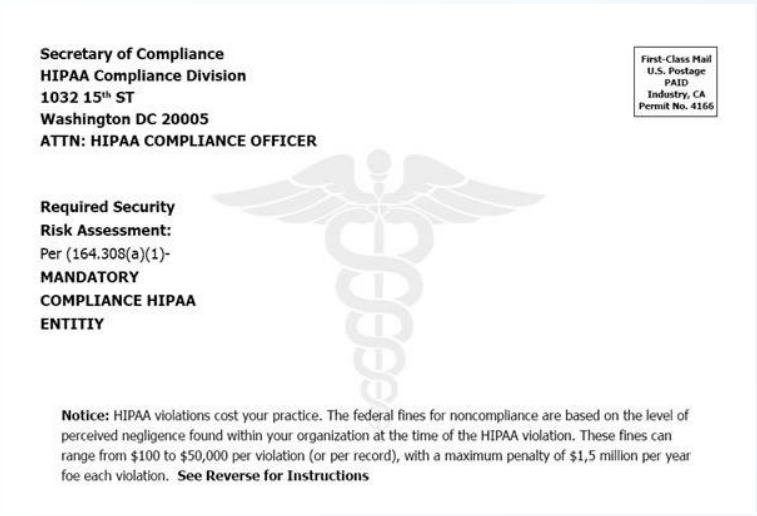
For more information related to HIPAA and COVID-19, please visit:
https://www.hhs.gov/hipaa/for-professionals/special-topics/hipaa-covid19/index.html

∞∞∞∞∞∞∞∞∞∞

Postcard Disguised as Official OCR Communication

OCR was made aware of postcards being sent to health care organizations disguised as official OCR communications, claiming to be notices of a mandatory HIPAA compliance risk assessment. The postcards have a Washington, D.C. return address, and the sender uses the title "Secretary of Compliance, HIPAA Compliance Division." The postcard is addressed to the health care organization's HIPAA compliance officer and prompts recipients to visit a URL, call, or email to take immediate action on a HIPAA Risk Assessment. The link directs individuals to a non-governmental website marketing consulting services. A copy of the postcard is on the next page (page 5). If you receive such a post card, disregard it, and refrain from visiting the websites it promotes.

Continued from page 4

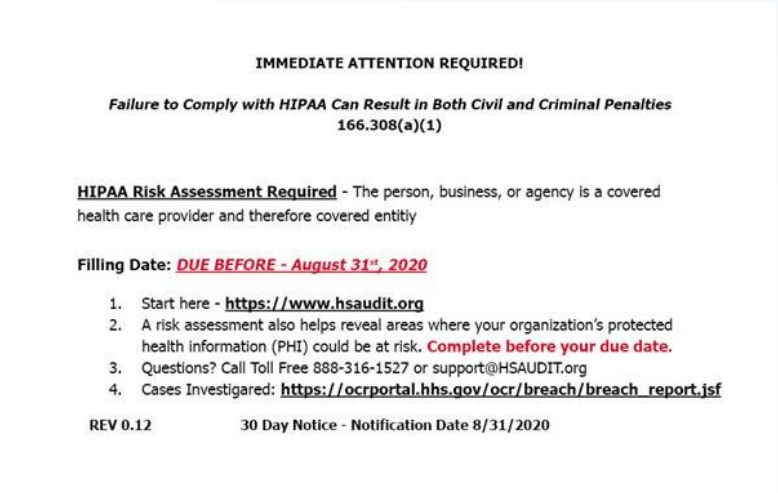


Secretary of Compliance
HIPAA Compliance Division
1032 15th ST
Washington DC 20005
ATTN: HIPAA COMPLIANCE OFFICER

First-Class Mail
U.S. Postage
PAID
Industry, CA
Permit No. 4166

Required Security Risk Assessment:
Per (164.308(a)(1)-
MANDATORY COMPLIANCE HIPAA ENTITIY

Notice: HIPAA violations cost your practice. The federal fines for noncompliance are based on the level of perceived negligence found within your organization at the time of the HIPAA violation. These fines can range from $100 to $50,000 per violation (or per record), with a maximum penalty of $1,5 million per year foe each violation. **See Reverse for Instructions**



IMMEDIATE ATTENTION REQUIRED!

Failure to Comply with HIPAA Can Result in Both Civil and Criminal Penalties
166.308(a)(1)

HIPAA Risk Assessment Required - The person, business, or agency is a covered health care provider and therefore covered entitiy

Filling Date: ***DUE BEFORE - August 31st, 2020***

1. Start here - **https://www.hsaudit.org**
2. A risk assessment also helps reveal areas where your organization's protected health information (PHI) could be at risk. **Complete before your due date.**
3. Questions? Call Toll Free 888-316-1527 or support@HSAUDIT.org
4. Cases Investigared: **https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf**

REV 0.12 **30 Day Notice - Notification Date 8/31/2020**

All UBMD staff members should be alerted to this misleading communication. This communication is from a private entity, NOT from HHS/OCR. You can verify that a communication is from OCR by looking for the OCR address or email address. The addresses for OCR's HQ and Regional Offices are available on the OCR website at https://www.hhs.gov/ocr/about-us/contact-us/index.html, and all OCR email addresses will end in @hhs.gov.

Suspected incidents of individuals posing a federal law enforcement, or any other suspected HIPAA violations, should be reported to the UBMD Compliance Office immediately.

"It takes less time to do things right than to explain why you did it wrong."

~ Henry Wadsworth Longfellow

HHS Office for Civil Right (OCR) Alert: Individual Posing as OCR Investigator

The HHS OCR recently posted the following alert:

It has come to our attention that an individual posing as an OCR Investigator has contacted HIPAA covered entities in an attempt to obtain protected health information (PHI). The individual identifies themselves on the telephone as an OCR Investigator, but does not provide an OCR complaint transaction number or any other verifiable information relating to an OCR investigation.

HIPAA covered entities and business associates should alert their workforce members, and can take action to verify that someone is an OCR investigator by asking for the investigator's email address, which would end in ***@hhs.gov****, and asking for a confirming email from the OCR investigator's hhs.gov email address.*

Suspected incidents of individuals posing as federal law enforcement should be reported to the Federal Bureau of Investigation (FBI). The FBI issued a public service announcement (PSA) about COVID-19 fraud schemes at:

https://www.ic3.gov/media/2020/200320.aspx

The UBMD Compliance Office strongly recommends that you follow the above link and read the PSA, so that you will not be caught off guard. Please contact the Compliance Office with any questions, or if you suspect your practice may have been affected by COVID-19 fraud, or any fraud.

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

Beverly A. Welshans, CHC, CPMC, CPC, CPCI, COC, CCSP
Director of Audit & Education
716.888.4702
welshans@buffalo.edu

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

UBMD COMPLIANCE HOTLINE: 716.888.4752

Report suspect fraud/abuse, potential problems,

or HIPAA concerns.

Ask questions or request guidance | Provide relevant information.

Remain anonymous if you wish | Non-retaliation policy will be adhered to.

(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:

2020 Second Quarter Quiz

---

1. According to UBMD policy:

   A. No PHI may be stored on laptops.
   B. No PHI may be stored on phones.
   C. All new laptops must be encrypted in case stray PHI finds its way onto the hard drive.
   D. All of the Above

2. The unencrypted electronic distribution of PHI in text messages or email is prohibited.

   A. True
   B. False

3. According to the 2021 CPT E/M changes, which of the following statements is incorrect?

   A. There will be no required level of history or exam for visits 99202-99215.
   B. Time no longer has to meet 50% rule nor be dominated by counseling.
   C. New and established patient visits can be based only on time.
   D. Code 99201 will be deleted.

4. Visits will have a range for time, For example, 99213 will be 20-29 minutes; 99214 will be 30-39 minutes.

   A. True
   B. False

5. Which of the following is correct?

   A. Even during the COVID-19 public health emergency, covered health care providers are still required to obtain a valid HIPAA authorization for each patient whose PHI will be accessible to the media before media is given access.
   B. The HIPAA Privacy Rule does not permit providers to give media and film crews access to facilities where patients' PHI will be accessible, without the patients' prior authorization.
   C. Reasonable safeguards that should be used to protect patient privacy whenever the media is granted access can include installing computer monitor privacy screens, and setting up opaque barriers to block the film crew's access to the PHI of patients who didn't sign an authorization.
   D. All of the above are correct.