Overview of HIPAA in Dentistry: The Basics

Welcome to today's course, *Overview of HIPAA in Dentistry: The Basics*. Thank you for taking the time out to join us today. So let's see what we have in store, as we guide you through some of the key features of this crucial piece of legislation.

1. First of all, let's look at an accessible, user-friendly definition of HIPAA;
2. Secondly, it's important to be familiar with the purpose of this policy;
3. We can then move on to look at any misunderstandings we may have regarding HIPAA;
4. Some common scenarios will hopefully exemplify HIPAA in everyday practice;
5. Logically, this will be followed by some practical advice as to how to adhere to HIPAA guidelines in your work environment;
6. In the unlikely event – hopefully! – that you find yourself in violation of HIPAA, you need to be armed with knowledge of potential penalties;
7. Finally, we'll finish up with a few quiz questions to ensure you folks have been taking note!

What is HIPAA?

HIPAA, sometimes referred to as Public Law 104-191, is an acronym for the Health Insurance Portability and Accountability Act. On August 21st 1996, having been passed by Congress, it was signed in to law by the then president, Bill Clinton.

It is sometimes helpful to examine individual words within a pretty long-winded concept in order to grasp its essence. So let's chunk the title of this Act down a little:

Insurance: This is essentially a contract which guarantees protection against a defined set of risks. In the world of health – in our case, dentistry specifically – it protects the individual against unemployment, negligence and the like.

Portability: At its most basic level, this means the ability to be carried around. Here it refers to the possibility of insurance being transferred from one system to another – for example, the patient has access to that insurance if they shift from one dental practice to a different provider. The guidelines apply nationwide.

Accountability: To be accountable is to be responsible and liable. Every dental provider, therefore, has a duty to protect their patients not only on a clinical level, but in relation to their personal data.

Why Is HIPAA Needed?

So, primarily HIPAA's purpose is to combat abuse. This legislation was developed as a response to an increase in data breaches, cyber-attacks and ransomware. Back in 1996, as technology became more sophisticated, it became clear that the

security of personal data needed to be strengthened. In the litigious world we live in, such breaches can be a costly business for providers of care. I guess we could say that HIPAA is a reaction to the modern world.

A Word of Caution

This is really a linguistic issue! Even among professionals, it is quite common to misspell HIPAA as HIPPA. No harm done, of course, unless you type this into a search engine – the results will tell you that HIPPA refers to a decapod crustacean, the *Hippidae*! It's a matter of professionalism that we get it right: this could be through a simple matter of splitting the acronym in two (Hip – AA) or coming up with memory-jogging mnemonic. Here's a basic one:

Health

Is

Pretty

Awesome,

Actually.

Or you might prefer the somewhat 'loftier':

Hippocratic

Integrity

Pervades

All

Activity.

This may seem like a minor misunderstanding, but evidence suggests that up to a quarter of professionals get this wrong, even in legal documents! Let's get this simple thing right.

Some Key Features

So we're now going to take a look at some of the key characteristics of HIPAA and anticipate some of the questions dentists – particularly new dentists – may have. Remember, the information covered today is not exhaustive – as a practitioner, it is a requirement that you delve into the document itself. Not great bedtime reading, I know – but needs must, as they say. What follows is some key information you may or may not be familiar with:

- It is permissible for each state to have its own discrete ruling regarding the release of patient records. Of course, it's up to you to familiarize yourself with

the particulars of the state in which you operate – and to ensure that you share this knowledge with your employees.

- Federal HIPAA law only outlines the basic minimum requirements; there is absolutely no reason why you can't supplement these guidelines with even tighter, stricter practices of your own.
- In the unfortunate (but realistic) event that a patient expires, records can only be released to an individual presenting a short certificate, which provides evidence that they are responsible for the estate - or to a person known to be responsible for the payment of the patient's care.
- If a patient requests 'all' of their records, then the following *must* be provided: charts. ledgers and account notes; x-rays; periodontist charts; a full list of disclosures; generally, all documents, including images. In this case, interpret 'all' as to mean *every* piece of documentation in existence.
- In terms of record release, if a patient moves from one state to another the 'whichever is less' policy applies. If, for example, the patient moves from a state which has a 40 day release policy to a state where the policy decrees a 30 day release period, then the records must be supplied within 30 days. So be sure of the ruling of the state a patient has moved on to – it may well be different from your own. Don't get caught out.
- Any training you carry out in your practice needs to be specific to any policies in place in *your* clinic. CEDR's annual online training is not compliant in itself; it's down to *you* to ensure that your employees are fully compliant with procedures regarding data protection and surgery practices.

Common Scenarios

No doubt about it, you and your staff make decisions every single day that are affected by privacy law. Knowing the guidelines is all well and good, but how do they translate into the real world? Let's take a look at a few scenarios:

<u>Scenario One</u>:

You call your receptionist into your office for a moment. He or she leaves their desk, which is clearly in the reception area. There are two patients waiting, located in reasonably close proximity to the desk. The reception will only be away from his or her station for three minutes tops. They make the decision to leave the computer as it is, given that there is hardly anyone around. Bad decision! Now, we all know that the likelihood is that absolutely nothing untoward will take place, right? Nevertheless, the opportunity for a data breach here is clear. The receptionist doesn't know for sure that one of those two patients won't just hop over to the desk and either retrieve or doctor data. It doesn't take long! Encourage safety measures to become habitual, minimizing risk and saving a whole lot of hassle all round.

<u>Scenario Two</u>:

A local celebrity visits your dental practice. Star-struck, your receptionist requests a photo with the celebrity and later posts said photo on social media. Consequently,

the celebrity's lawyer calls you, informing you of his/her client's intention to pursue this invasion of privacy with the OCR (Office of Civil Rights). Since the celebrity did not issue authorization, you – as opposed to the receptionist – could he held in violation of HIPAA under 45 CFR 164 506 *et seq*. This highlights the importance of ensuring all employees have access to training and read practice policy forensically.

Scenario Three:

A patient calls, complaining of swollen, bleeding gums. They would like to send a picture via mobile phone. Would this contravene HIPAA directives? This one is slightly ambiguous: the HIPAA Security Rule stipulates that protective measures must be taken by the provider to offset the inherent risks of transmitting information via mobile devices. If your practice has a signed document from the patient (and this is always a good idea) and there are muscular policies and procedures in place, then this mode of transaction would be permitted. Many practices do enjoy the convenience of this method of communicating with patients. Take note, however: sending texts to patients is another matter altogether – this is where your technical safeguards – more of this later – come into play.

Quite often, common sense wins the day – but, as a rule of thumb, in cases of doubt or uncertainty: check, check, check!

Practical Considerations

There is a saying in Russia that goes something like this: 'The fish rots from the head'. This metaphor roughly translates as 'leadership is the cause of an organization's failure'. This means that you, as clinicians, are accountable for any malfeasance that takes place under your roof. It is down to you to ensure that your place of business is HIPAA compliant and that all personnel are trained to an acceptable standard. So where do you start? Once you are fully familiar with the intricate details of HIPAA, it's time to ensure that they are applied to good effect in your practice. These procedures should become habitual, and can basically be broken down into three categories: physical, technical and administrative.

Physical Safeguards

- ✓ Make sure that your policies make it clear as to how data is stored, where data is stored, and who has authorized access. Who has full access? Who has limited access?
- ✓ In line with this, it is imperative that your policy is very *specific* about who has access: they should be identified by name and job title or function. This is not limited to on-site employees but should also cover contractors, business associates and so forth.
- ✓ Policies must explicitly state the methods you employ to maintain security regarding access. These methods can include computer access measures,

video surveillance, lockable areas, or human resources such as security guards.
- ✓ Consider contingency planning for situations such as loss of power in the building and the necessity of data restoration.
- ✓ Consider property control measures, such as the engraving of items.
- ✓ Consider issuing your employees and visitors with ID badges.

Remember, when considering physical safeguards, the term 'physical' does not only apply to the interior of your practice, but the exterior and its environs.

Technical Safeguards:

It seems that the world is increasingly technology-driven on an almost daily basis. The challenge that comes with all this wonderful innovation is the extent to which organizations can protect their patients' privacy. It may seem that in the age of social media and the proliferation of online platforms for sharing that privacy is an alien concept. Yet when it comes to our most personal information, privacy is exactly what patients want and expect. As with physical documents, EPHI (electronic protected health information) records must be rigorously protected. How can you take measures to fulfil this requirement, then?

- ✓ Access control is crucial: this can be exercized through unique user identification, automatic logoff, and encryption and decryption. Be really clear as to which employees require access to hierarchical levels of information.
- ✓ Consider the *integrity* of EPHII data – could you implement an electronic signature, for example? Electronic data is highly vulnerable, so it is an investment to look into functions that maximize protection.
- ✓ Anticipate scenarios whereby the transmission of EPHI renders it open to corruption. How do you strategize such instances? Look into this one carefully. It can come back and bite you!

Administrative Safeguards:

This refers to things like policies and procedures, staff training programmes and auditing and monitoring. How effective are your Risk Assessments? Have a look at this checklist. Are all of these procedures accounted for in *your* practice?

- ✓ Your policies should include key information as to how you hire and dismiss employees. Is it really clear, in your documentation, which employees have access to sensitive information and which don't? Consider who is responsible for specific data-related tasks such as calling patients, inputting data, system updates, et cetera, All of the factors covered in the 'physical' and 'technical' sections should be documented and communicated in written form. A good starting point might be to list every task that is carried out within the practice – to whom is each task assigned? What level of access to information do they have? How do you

ensure that employees who leave do not pose a security risk? Is their access to your electronic systems disabled? Have you ensured they no longer have unrestricted access to the building? It may be that you need to rip up existing policies and create new ones. There's no room for ambiguity here! Systemic problems that are not addressed can lead to costly and embarrassing solutions.

- ✓ In terms of training, consider how you stay up to date with HIPAA compliance regulations. Do you regularly read updates? Do you attend training of some form? Remember what we said about that fish!
- ✓ It is your responsibility to ensure that new employees are fully trained in HIPAA. You may delegate that – officially – to a member of your team, or perhaps enrol your new people on a local or online training programme. Just make sure they are made explicitly aware of how the guidelines are implemented in your specific business.
- ✓ Do you ensure that your established employees have access to refresher training? This is the kind of thing that really should be embedded in your written policies, too.
- ✓ How do you audit and monitor what goes on in your practice? Are you able to track employee activity on your network? It's time to get tech-savvy – or employ someone who can!
- ✓ Make sure that all employees sign Confidentiality Agreements. It's a good idea to formulate a carefully-worded agreement for patients to sign, too.

Violation and Penalties

We mentioned earlier that it's a good idea to read, or reread, the legislation. Hopefully, you are so clued up that the concept of violation penalties is not even on your radar! However, if you're looking for motivation to read the thing, then look no further:

- ! Negligence can incur a fine ranging from $100 to$50.000! And that's per violation or record! Fines are capped at $1.5million per year. Worth bearing in mind!
- ! Some violations can lead to jail time. That will give you plenty of time to sit back and read that legislation…
- ! Finally, and crucially, a price cannot be pinned on the damage to your reputation. The thought of being plastered on that OCR digital 'Wall of Shame' should give you cause to think twice before risking even the most minuscule indiscretion. Don't even go there!

The good news is that most of the safeguarding requirement written into HIPAA are common sense, so shouldn't be too difficult to implement. In case you didn't already know, if a transgression is brought to your attention in your practice you must submit a breach report through the OCR website. You must also notify any affected individuals and the federal government. If the number of individuals affected

exceeds 500 you are duty bound to inform the media too. *Not* the kind of media attention you want!

Recapitulation and Conclusion

Hopefully, some of the information we've provided on this course will help keep you out of hot water! Before you go, let's just test your recall about this very important topic by taking part in a short quiz. Thank you again for joining us today.

Quiz

1. HIPAA became law in which year:
    a) 1995
    b) 1996
    c) 1997
2. Which president signed the legislation into law?
    a) Bill Clinton
    b) George Bush Sr.
    c) George Bush Jr.
3. Approximately how many professionals spell the acronym incorrectly?
    a) A fifth
    b) A third
    c) A quarter
4. If a patient transfers to another state, what is the rule regarding the time-frame for releasing records?
    a) Whichever number is more
    b) Whichever number is less
    c) Whichever number you prefer
5. What are the three categories of safeguarding measures?
    a) Physical, Virtual and Administrative
    b) Physical, Technical and Digital
    c) Physical, Technical and Administrative
6. What does EPHII stand for?
    a) Electronic personal health information
    b) Electronic protected health information
    c) Electronic portable health information
7. Following a violation of HIPAA, how many individuals have to be affected before the media is informed?
    a) 50
    b) 500
    c) 5000

Answer Key

1. HIPAA became law in which year:
    a) 1995
    b) 1996
    c) 1997
2. Which president signed the legislation into law?
    a) Bill Clinton
    b) George Bush Sr.
    c) George Bush Jr.
3. Approximately how many professionals spell the acronym incorrectly?
    a) A fifth
    b) A third
    c) A quarter
4. If a patient transfers to another state, what is the rule regarding the time-frame for releasing records?
    a) Whichever number is more
    b) Whichever number is less
    c) Whichever number you prefer
5. What are the three categories of safeguarding measures?
    a) Physical, Virtual and Administrative
    b) Physical, Technical and Digital
    c) Physical, Technical and Administrative
6. What does EPHII stand for?
    a) Electronic personal health information
    b) Electronic protected health information
    c) Electronic portable health information
7. Following a violation of HIPAA, how many individuals have to be affected before the media is informed?

a) 50
b) 500
c) 5000

Sources

https://www.hipaajournal.com/hipaa-rules-for-dentists/

hhs.gov

https://www.dentistryiq.com/practice-management/patient-relationships/article/16366021/emails-texts-and-hipaa-7-rules-every-dentist-needs-to-know

https://www.revenuewell.com/article/dental-hipaa-questions-answered/

https://www.atlantic.net/hipaa-compliant-hosting/hipaa-compliance-guide-what-is-hipaa/