HIPAA: Bigger and More Annoying

Instructor: Laney Kay, JD

Contact information:

4640 Hunting Hound Lane
Marietta, GA 30062
(770) 312-6257
(770) 998-9204 (*fax*)
laney@laneykay.com
www.laneykay.com

OFFICIAL DISCLAIMER
from Laney Kay

President, Entertaining Training, LLC
(*now necessary because someone pitched an absolute hissy fit)*:

This program is intended to provide general information about HIPAA regulations and you will receive continuing education credit. In addition, this program is intended only to offer general guidance regarding HIPAA privacy, security, and HI TECH breach information, and other related topics; any suggestions offered by me are only my opinion and should not be construed as advice, legal or otherwise. Any specific questions, circumstances, or situations you are concerned about in your particular office should be addressed by your own attorney. Nothing I say is intended to establish a standard of care or industry custom. No one, including me, can "HIPAA-proof" an office and nothing said in this program will reduce your likelihood of a HIPAA-related inspection, nor will it prevent you from getting fined, nor will it reduce the amount of the fine in the event of an inspection.

AND NOW FOR THE NOT-AS-OFFICIAL DISCLAIMER...

Any other information is intended for entertainment purposes only, and I'll apologize now in the event you don't find me entertaining. Nothing said is intended to offend you or any attendee, and I apologize if you are offended in any way.

AUTHORIZATION TO RELEASE PROTECTED HEALTH INFORMATION

I authorize the use or disclosure of the protected health information ("PHI") as described below. By authorizing the use or disclosure of the PHI described below, I authorize the custodian of the PHI

(1) to open the PHI for review or inspection by the person(s) identified below, and (2) to furnish the person(s) identified below with a copy of the PHI if he or she so requests.

Patient Name: _____

DOB: _____

Description of PHI requested : any and all contents of dental record, including diagnosis, treatment details and financial information.

I authorize _____ (*ofc name*) to release and/or disclose the PHI described above to the following person(s) :

The purpose of this request to release and/or disclose the PHI described above is for personal reasons. I understand that I have the right to revoke this Authorization, in writing, at any time by notifying the office above. Such revocation will not affect actions taken by the requesting person prior to the date he or she received the written revocation. I also understand information disclosed pursuant to this authorization may be subject to redisclosure by the recipient and will no longer be protected by this rule.

I understand that my health care provider cannot condition treatment on whether I sign this Authorization. However, if I refuse to sign this Authorization, I understand that I will be financially responsible for any dental work provided by this office.

This Authorization will expire at such time that:

___ I become financially responsible for all dental work performed by this office; or
___ The following date: _____ (*within one year of current date*).

_____ _____
Signature of Patient Date

Personal Health Information Release Form
(HIPAA Release Form)

Name: _____ **Date of Birth:** _____/____/_____

Release of Information

[ ] I authorize the release of any and all information including the diagnosis, financial and dentalrecords; examination rendered to me and claims information. This information may be released to:

[ ] Spouse_____
[ ] Child(ren)_____
[ ] Other_____
[ ] Information is not to be released to anyone.

This ***Release of Information*** will remain in effect until terminated by me in writing.

Messages

Please call [ ] my home [ ] my work [ ] my cell Number:_____

If unable to reach me:

[ ] please leave a detailed message
[ ] please leave a message asking me to return your call
[ ] _____

The best time to reach me is (*day*)_____ between (*time*)_____

I understand that this office will try to accommodate my wishes about my contact information, but may have to contact me at the other numbers if unable to contact me at my requested number/location.

Signed: _____ Date: ____/____/_____

Authorization for Release/Use of Protected Health Information In the Form of Photos, Radiographs, and Electronic Images

Name of office: _____

Your photos and x-rays are part of your diagnostic and clinical record and are considered to be protected health information under federal HIPAA Privacy Laws.

We make use of radiographs (x-rays), photographs, and digital images. These images may be used for diagnosis, documentation, reference, teaching, and research publication. Some cases that present exceptional results, particularly remarkable smiles, or interesting situations may be utilized for demonstration, education or advertising to potential and existing patients in our office either in print media, television, on digital media and on our webpage. In some instances, you may be recognizable in some of these images.

By initialing and signing this form, you are authorizing us and releasing us from any liability resulting from the use/release of such images. Your authorization and release to use images will in no way affect the quality of your results in our office. We do our best to provide exceptional dentistry to all patients.

___ I authorize the use of my images where my face is identifiable
___ I authorize the use of my images where only my teeth are identifiable
___ I authorize the use of my radiographs

The purpose of this request to release and/or disclose the PHI described above is for personal reasons. I understand that I have the right to revoke this Authorization, in writing, at any time by notifying the office above. Such revocation will not affect actions taken by the requesting person prior to the date he or she received the written revocation. I also understand information disclosed pursuant to this authorization may be subject to redisclosure by the recipient and will no longer be protected by this rule.

I understand that my health care provider cannot condition treatment on whether I sign this Authorization. This Authorization will expire at such time that:

___ I determine that I no longer wish for my images to be used and I revoke this authorization in writing; or
___ The following date: _____ (*within one year of current date*).

_____ _____
Signature of Patient Date

In order to comply with the HIPAA Security Rule, all covered providers must have regular risk assessments to ensure that their patients' private health information is as safe as possible. Although you probably completed a comprehensive risk analysis at the time the HIPAA policies were first implemented, risk assessment is an ongoing process. Here is a sample risk analysis you can use that is based upon a document from HHS designed to help small providers with HIPAA security compliance. We all make changes in our offices that can result in compromising the security of patients' information; regular risk assessments help us ensure that we keep the information as safe as possible.

The standard requires that we regularly assess administrative, technical and physical safeguards to ensure compliance with the HIPAA rules. This form will help you perform regular checks. Please note this is a sample risk analysis that you may use to formulate your own policies and risk assessments, and may not cover every situation that may exist in every office, so always check with your own attorney or malpractice carrier to make sure your assessment is complete.

Please fill out this form. For any actions that need to be performed, number the item, and at the end, fill out the actions that must be taken for each numbered item on the attached action plan.

Administrative Safeguards	Yes	No	Needs to be addressed	Item # on action plan
General office information				
Have you conducted a thorough risk analysis to determine potential risks and vulnerabilities to the safety of patient's electronic private health information (PHI)?				
Do you have a security and/or privacy officer in charge of the HIPAA program? Name(s):				
Do you know where PHI is located in the office? Please underline all that apply: desktop computer , laptop computer, tablets, smartphones, server, flash drive, removable hard drives, CDs, paper charts, other: _____				
Do you have a current inventory of all technical items that may contain patients' PHI?				
Do you know the approximate value of all technical items that may contain patients' PHI?				
Have you taken reasonable security measures to protect your patient's information, including door locks, the use of passwords, security systems, and other measures to ensure that PHI is secured?				
Do you have a current backup in the event of a natural disaster so that your patients' information can be easily restored?				
Do you have control over the information on your computer system?				
Business Associates				
Does any vendor or business associate have access to your computer system?				
Does any vendor or business associate have the ability to access and change confidential patient data? If so, are audit logs monitored to prevent unauthorized access?				
Do you have business associate agreements in place for all vendors who may have access to your patients' PHI?				
Do these agreements have assurances that these business associates will properly protect patients' information?				
Do you use a clearinghouse, and if so, do they take precautions to protect your patients' information during processing and transmission?				
Do these agreements include indemnification agreements in the event a breach is caused by a business associate?				

Administrative safeguards (continued)	Yes	No	Needs to be addressed	Item # on action plan
Employee Information				
Have your employees received training on basic HIPAA requirements (Privacy, Security, HITECH, and Omnibus Acts)?				
Do you provide additional training if new policies and procedures are implemented?				
Do you document all employees training?				
Do you have written policies and procedures that explain employee requirements under HIPAA?				
Do you contact references and/or conduct background checks before hiring employees?				
Do employees know where the HIPAA manual is kept?				
Do all employees understand there are specific sanctions for violating HIPAA Privacy and Security policies (including being fired) and that all sanctions will be enforced?				
Do all employees understand that, in addition to workplace sanctions, they can also be fined and imprisoned for deliberately violating HIPAA rules?				
Do only those employees, who need access to patients' PHI, actually have access to PHI? (Those without authorization, should not be able to access patients' information)				
Does each employee have a specific log in ID?				
Do you use passwords on your system to prevent unauthorized access?				
Are employees trained not to share passwords or leave them in places that are easily accessible?				
If you have any employees who are not authorized to access patients' PHI, could they access it?				
Do terminated employees still have access to your computer system or do you have systems in place to prevent that scenario?				
Are locks/passwords/etc. changed to prevent continued facility access after termination?				
Do you periodically review employees' access to PHI as needed? (If they change to a job that no longer requires access to patients' PHI, they should no longer have access)				
If any employees can access your system using their personal devices, are they aware of encryption requirements?				
If any security/privacy lapses among employees occur, is additional training and instruction provided?				
Do new employees receive training about the HIPAA programs and are informed about policies, sanctions, etc.?				
Do employees know to inform the HIPAA officer immediately if they suspect information has been compromised?				
General computer protection information				
Would you know if someone was trying to hack into your system?				
Do you have audit logs that may show unsuccessful log-ins or other indicators of unauthorized access?				
Are passwords protected and changed when indicated?				
In the event of computer destruction or loss, are there policies and procedures to restore computer service and restore data (does everyone know who to call)?				
Do employees know they should not install personal software or access personal e-mails on the office computer system because of the potential for viruses and malware?				
If you offer patients Wi-Fi in your office, is their access on a separate router to prevent access to your system?				
Do you perform regular risk assessments and security evaluations, at least annually or any time a change is made?				

Administrative safeguards (continued)	Yes	No	Needs to be addressed	Item # on action plan
Do you have firewalls, anti-viral software, etc. to protect your information from malware/spyware/viruses? (If you use a computer expert, have him write a summary of precautions you've taken to place in your HIPAA manual)				
Are any security incidents documented?				
Do you backup your data?				
Is your data stored offsite in the event the office is destroyed? (What if your home is destroyed at the same time? You should have data backed up in a manner that will provide for widespread devastation to a large area.)				
Do you have a plan that will allow you to temporarily relocate if your office is damaged?				
In the event you're in a temporary location, could patients' information be adequately protected?				
Do you have copies of existing software in the event you have to replace a computer?				
If you make changes to your computer system or relocate computers in the office, do you evaluate the situation to ensure that the new changes do not compromise security? (For example, you move a computer to a consult room and patients may have unsupervised access in that room; passwords, etc. would be very important on that computer).				
Physical Safeguards				
Is your facility protected from unauthorized physical access? (Do you have door locks, cameras, alarms, physical safeguards preventing computer removal, locked cabinets, etc?)				
If hardware, doors, locks, walls, etc. are repaired or modified, are any changes that could affect the security of PHI should be documented?				
Do you use screen savers, privacy screens, etc. to ensure that patient information isn't easily visible to others?				
Are computers placed to ensure that patients' PHI isn't easily visible to others?				
Are computers placed to ensure that unauthorized people don't have unsupervised access? (And if they are unsupervised, is there adequate protection to ensure that other patients' information can't be accessed?)				
Do unattended computers automatically log off when not being used?				
If computers or electronic media are no longer being used/are being replaced, is there a method that destroys the data before disposal?				
Are all flash drives, hard drives, etc. all accounted for and it is known who has them in their possession at all times?				
Is data consistently backed up?				
If data is backed up to a physical item such as a CD or flash drive, how are they protected, stored and destroyed?				
Technical Safeguards				
Since each employee has a unique identifier in the computer system, could their activities be tracked in the system?				
Are passwords unique and not shared?				
Are employees notified that they may be sanctions if they share passwords or use someone else's identifier?				
Do employees have access to only the minimum PHI necessary to do their job duties? (This is usually not relevant in most dental offices where those who have access need access to everything; however, some larger practices do have separate departments for billing, etc.)				
If specific emergency procedures are in place that require certain codes for PHI access, are the codes protected and available only to those who need them?				

Technical safeguards (continued)	Yes	No	Needs to be addressed	Item # on action plan
If you have automatic logoff for computers, does the time before it logs off shorten for those computers in high traffic areas?				
Do you use e-mail in the office to transmit PHI?				
Do you have a method to encrypt e-mails if it's used to transmit PHI?				
Are other methods of protecting documents, such as password protection of individual documents, used?				
If a patient requests information and the doctor/employee doesn't have access to the encrypted email address to transmit the information, do the doctor and employees know they can request patient permission to transmit using an unencrypted e-mail and then transmit only if permission is granted?				
Are users denied access after a certain number of failed log-in attempts?				
Does the doctor and/or security officer know how to conduct audits for altered information, failed log-ins, etc.?				
Are charts or electronic devices ever taken out of the office (including backup devices, smart phones, etc.)?				
Is your electronic PHI protected by encrypting your information? (Encryption is the only method that will actually render electronic information "unusable" which can avoid a breach in the event your information is accessed, lost, or stolen.)				
If your information is not encrypted, do you have encrypted passwords?				
Are any electronic portable devices that can access patients' information encrypted?				
Do your employees know to immediately report any suspected breaches of information?				
Do your business associates know to immediately report any suspected breaches of information and provide you with all needed information to determine if a breach has occurred?				
Do your business associate agreements have specifics about how breaches will be handled, and are indemnification agreements in place to ensure that notification and mitigation costs will be covered?				
General Privacy Provisions				
Do employees understand the necessity of disclosing the "minimum amount necessary"?				
Is there personal health information on the outside of patients' charts?				
Are paper charts inaccessible to unauthorized people?				
If sensitive matters are discussed, is there a place to take patients for a more confidential discussion? (Note: never close yourself in a room with just you and a patient. Always bring in another person or leave the door cracked and put someone outside the door to protect you from any false claims or accusations.)				
Do you have authorizations that will allow you to discuss dental and financial matters with those who are financially responsible for others?				
Do employees know never to discuss patients outside the office?				
Are schedules posted in a non-obvious location?				
On sign in sheets, do you ensure that no personal information is asked such as "what is your dental problem today"?				
Is the "Notice of Privacy Policies" posted and available to patients, and did patients sign a form acknowledging receipt?				
Do employees understand that PHI cannot be used for personal reasons?				
Have patients signed authorizations for any photos/xrays used in your office? (before/after pictures, etc.)				

Action Plan

Item # on Risk Analysis	Actions that need to be taken	Date Completed

Breach Risk Assessment

Date of Incident (or Notification Date):	**Number of individuals affected:**
Summary of Events:	
1. Type of Information (names/social security/credit card numbers/clinical information/medical history):	
2. Who received/used the information:	
3. Was the information actually acquired or viewed (explain):	
4. Has the risk been mitigated so that the entity is assured the information will not be used (and if so, how?):	
After completing the risk assessment, it has been determined: **___This is a breach requiring notification, and breach requirements will be followed ; OR____ This is not a breach and notification is not necessary**	