PCC's Recommended Guidelines for a HIPAA Privacy Policy

As you create or update your practice's HIPAA Privacy Policy, keep these important features in mind.

Your HIPAA Privacy Policy should state that a patient's private PHI should not be used or disclosed to anyone other than the patient except in certain circumstances.

Your policy should outline when it *is* appropriate for your staff to share PHI with other individuals that are not the patient without permission.

- PHI may be shared when required by law, if by subpoena or other court order.
- PHI must be released to the proper authorities if abuse, neglect or domestic violence is suspected.
- PHI may be shared when required for public health purposes for public health surveillance, investigations and interventions.

Next, your HIPAA Privacy Policy should describe how you implement internal privacy policies and procedures. The policies and procedures should include:

- How to properly dispose of PHI that may be printed or saved to an external drive (ie: shredding a piece of paper with PHI, shredding a CD that contains PHI)
- The importance of not sending any PHI over email unless the message is encrypted
- The HIPAA "minimum necessary" guideline: only give people the minimum amount of information that is needed to perform their job.
- Ensure employees know the difference between PHI and IIHI (Individually Identifiable Health
- Information). Even though there is a difference, both are protected under the HIPAA Privacy rule.
    - PHI: Health information for the patient ie: diagnosis codes, billing information, assessment notes
    - IIHI: Patient personal information ie: address, social security number, date of birth

Your HIPAA Privacy Policy should also state that you will train employees to understand these policies and procedures as appropriate for their functions.

The policy should designate individuals who are responsible for implementing privacy policies and procedures, and who will receive privacy-related complaints.

Finally, your privacy policy should state that you will have in place appropriate administrative, technical, and physical safeguards to protect the privacy of health information.