This newsletter is one in a series that provides general information on key components of the HIPAA Privacy and Security Regulation. More detailed information and policies are available on the MCW HIPAA website. In this newsletter we’ll cover information about patient health information use and disclosures for treatment, payment and operations, and research.

**Treatment, Payment and Operations** - To avoid interfering with an individual’s access to quality health care or the efficient payment for such health care, the Privacy Regulation permits a covered entity to use and disclose protected health information (PHI), with certain limits and protections, for treatment, payment, and health care operations (TPO).

In general the Privacy Regulation allows the College to use PHI for our own TPO without first obtaining a patient’s authorization. This allows the College to see patients, generate bills and collect payments, and conduct specified operational activities:

- **Treatment** - means the provision, coordination, or management of health care and related services among health care providers or by a health care provider with a third party, consultation between health care providers regarding a patient, or the referral of a patient from one health care provider to another.

- **Payment** - encompasses the various activities of health care providers to obtain payment or be reimbursed for their services and of a health plan to obtain premiums, to fulfill their coverage responsibilities and provide benefits under the plan, and to obtain or provide reimbursement for the provision of health care.

- **Operations** - are certain administrative, financial, legal, and quality improvement activities of a covered entity that are necessary to run its business and to support the core functions of treatment and payment. Examples include quality assessment and improvement; outcomes evaluation and clinical guidelines; protocol development; case management; accreditation; certification, licensing, credentialing; training programs (e.g. medical students); or compliance activities.

**Research** - The Privacy Regulation defines research as “a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.” The most common methods for accessing protected health information (PHI) in research are:

- **Patient Authorization** - Separate, explicit authorization is required from patients to use their protected health information for research activities. This authorization is typically included in the Informed Consent document. Under certain conditions an investigator may use protected health information for research without the patient’s explicit authorization, but these conditions require an IRB’s review and approval – e.g. “waiver of authorization” or “access to de-identified information.”

- **Waiver of Authorization** – Waiver of authorization may be granted by the IRBs to access PHI for research without a patient’s authorization. Legitimate reasons that the IRB may grant a waiver of authorization include:

  1. Research on Decedent’s Information: Where the PHI refers solely to deceased persons (the IRB may ask for documentation of death), and that such access is essential for the research.
  2. Reviews Preparatory to Research: PHI will not leave the covered entity, will be used solely for reviews preparatory to research (e.g. for protocol development), and the researcher represents to the IRB that such access is essential.
  3. Research involving retrospective data analysis or chart review.
  4. Identifying participants for recruitment for research by review of patient records or databases.
  5. Limited Data Sets: A researcher may enter into an appropriate data use agreement that has been reviewed and approved by the IRB.

- **Access to De-Identified Information** – A researcher may use PHI contained in a fully de-identified dataset. As the name implies, de-identified information must have all direct and indirect identifiers removed to eliminate re-identification using statistical techniques. There are 18 separate patient identifiers included in this requirement.

**Computer Security Tip:**

Whenever feasible, copy and paste e-mail addresses or use the e-mail reply button to limit misdirected e-mail.

You can reference additional information on HIPAA Privacy and Security at:
The MCW HIPAA website: [http://infoscope.mcw.edu/display/router.asp?docid=7961](http://infoscope.mcw.edu/display/router.asp?docid=7961)