CME Program Privacy Policy

It is the policy of the Case Western Reserve University School of Medicine CME Program to maintain the privacy of patients' Protected Health Information (PHI) and to abide by all state and federal privacy laws (including the Health Insurance Portability and Accountability Act of 1996 (HIPAA)). Of specific concern to CME providers are situations where PHI might appear in a presenter's written educational materials or audio/visual materials. For example, information attributable to a specific patient might be included in a written case study or verbal discussion of a case or might appear in a visual presentation such an x-ray or similar diagnostic image or test where patient identifiers have not been removed. Accordingly, PHI may not be present in any aspect of an educational presentation without a patient's written authorization (and such authorization must be HIPAA compliant after April 14, 2003). Prior to presenting a presenter must represent and warrant that he/she has HIPAA-compliant authorization for any PHI in the presentation or presentation materials or that he/she acquired such protected health information from a source that (a) obtained a HIPAA-compliant authorization which authorizes Presenter's use of PHI during the presentation; or (b) was not under a legal obligation to maintain the patient's confidentiality.

CME Program Confidentiality Policy

It is the intent of the Case Western Reserve University CME Program in conformance with University policies to prevent identity theft to maintain the confidentiality of any physician or healthcare provider information obtained or utilized by the CME Program in the course of registration for CME activities, participation as faculty, preparation and release of transcripts of activities for which credit has been earned, or any other CME Program function that involves confidential information. Such confidential information includes physician mailing address, last four digits only of the Social Security number (used as a unique identifier) and record of credit hours earned. All such confidential information will be (1) retained in a secure, password-protected electronic data base and filing system, (2) never displayed where it may be observed or recorded and (3) released individually only upon receipt of written authorization from the party requesting their own information. The sole exception to the above is the use of the last four digits of the Social Security number in printed class lists to assure that participants with identical names are able to appropriately register or sign in.