

HIPAA: DOES IT APPLY TO MY ORGANIZATION?

The quick answer: probably.

The Health Insurance Portability and Accountability Act of 1996 (“HIPAA” or “Privacy Act”) was created to address privacy standards regarding the maintenance and disclosure of an individuals’ health information. Unfortunately, HIPAA is extremely confusing and as a result, it is not followed by many entities or individuals who should have protections in place. This is likely because most mistakenly believe that HIPAA only applies to the medical profession. This misunderstanding could lead to significant liability.

HIPAA applies to health plans, health care clearinghouses, and to health care providers who transmit information in electronic form in connection with the Health and Human Services Department. Health plans include both individual and group health plans that pay for medical care. This encompasses employer provided benefits and records that may be maintained by employers. However, if the employer has less than 50 employees and the plan they provide to employees is established, maintained, and administered solely by the employer, HIPAA does not apply. In order to be excluded from the requirements of HIPAA, an employer must meet all of the criteria in the previous sentence. It is not enough that the employer has less than 50 employees.

HIPAA protects all individually identifiable health information. This includes past, present, and future physical and mental health information which contains information that can lead to the identity of the individual it relates to. If all identifying information is removed from the document, and there is no reasonable basis to link the record to an individual, then there is no restriction to disclosure. If identifying information is contained in the document, then protections should be in place to limit disclosure to the allowable instances. Allowable disclosure includes disclosure with a release from the individual, disclosure directly to the individual, disclosure between medical professionals and for payment to ensure quick treatment, and for certain litigation and public health matters.

In order to avoid an inappropriate disclosure, HIPAA requires minimum standards be in place to protect the information at issue. However, as is standard for most legislation of this nature, minimum standards are not clearly identified or defined by the Act. What can be determined from various sources in charge with enforcing HIPAA is that minimum standards include a designated employee or employees to deal with the sensitive information, training for that employee, notification procedures to individuals regarding their rights, storage guidelines, dissemination guidelines and destruction guidelines.

The question of whether you are required to comply with HIPAA, and the minimum standards needed, is a difficult one to determine as there are many exceptions to the rule, and just as many exceptions to the exceptions that make HIPAA apply when you think it may not. As a result, it is recommended that every employer or entity that may come in contact with an individuals’ private health information have minimum standards in place to protect not just that individual, but also the entity from potential liability for unintended violations of HIPAA.

Barbi L. Feldman, Esq.