



Managing Information Privacy & Security in Healthcare

Institutionalizing Responsibility

Introduction

The well-known maxim "Confidentiality is everybody's business," states the basic truth. Transforming this truism into practice requires institutional work and personal commitment. This toolkit provides models and methods for assisting healthcare providers and organizations to manage patient records as a broad institutional process, including the technical protection of the information system. In addition to these concrete methods, however, healthcare providers should institutionalize a sense of responsibility for maintaining patient confidentiality at all levels, including individual staff, program managers, and organizational administrators. Methods for binding these levels of responsibility together should be implemented. An illustration of the one approach for this is explained below in the case study "Trustee/Custodian Agreements" from Kaiser Permanente.

Individual Responsibilities

In the course of doing their daily work, individual staff will acquire medical, familial, financial, and other types of private information about patients. They should divulge such information only to authorized persons and for authorized purposes as required. They should never discuss such information outside the context of treatment, payment, healthcare operations, or for other activities authorized by the individual (e.g. research), or as permitted or required by law. The HIPAA Privacy and Security Standards require that all members of the workforce receive training on privacy and security. They should read and comprehend the organization's policies, procedures, and practices for data security and patient confidentiality. They should be individually responsible for seeking answers to questions and/or issues they do not understand in these processes including bringing ambiguous, incomplete, or erroneous policies, procedures, and practices to the attention of the organization's administrators. Success in discharging these duties merit positive notice in annual evaluations. The HIPAA Privacy and Security Standards require sanctions to be applied for failure to discharge one's individual obligations in maintaining patient confidentiality. These sanctions often lead to disciplinary action, including possible termination of employment.

Program Responsibilities

A healthcare organization's program directors, physicians, nurses, investigators and unit managers are responsible for creating and promoting a climate for maintaining the confidentiality of patient

information. Conditions favorable to such a climate include acting as role models in practicing good patient confidentiality practices; developing effective staff in-service training programs on patient confidentiality; promptly investigating and disciplining potential breaches of patient confidentiality; rewarding exemplary practices in maintaining patient confidentiality; developing and revising policies, procedures, and practices for patient confidentiality as needed; and communicating a sense of good confidentiality practices to patients. Success in creating and promoting a satisfactory climate for patient confidentiality merits positive notice in annual evaluation.

Organizational Responsibilities

The organization's central administration bears responsibility for supporting physicians, administrators, nurses and other members of the workforce in their efforts to maintain patient confidentiality. Such support includes participating in the development of jointly acceptable policies, procedures, and practices for maintaining patient confidentiality, assuring that the organization's management promotes a climate of patient confidentiality; affirming management's authority to investigate and discipline potential breaches of patient confidentiality; and including performance in maintaining patient confidentiality as a component of the staff's annual evaluation. Institutional officials should continuously reaffirm the importance of good patient confidentiality practices to the life of the healthcare organization.