ADOPTtoolkit
Accelerating Diffusion of Proven Technologies

Center for Technology and Aging

Compliance:

A Guide from the Medication Optimization Technology Toolkit

Description

If a technology-enhanced medication optimization intervention involves the management of electronic medical information, complying with privacy and security mandates is essential. To comply with security measures, certain policies, procedures and technologies must be in place. This guide outlines many of the essential administrative components intended to ensure security and maintain patient privacy.

Audience

Intended for use in the administrative organization and ongoing operation of a program to optimize medication use that involves the use of patient-centered technologies.

Helpful Tips

- Establish policies and procedures (P&P) around security, responsibilities, risks and system support.

1 Implement Policies & Procedures

What P&P should be established for the administration of the medication optimization program?

2 Integrate Technology Practices

Are the instruments of the program aligned with policy standards and clinical practices?

3 Understand the Regulatory Landscape

Federal, state and locals laws influence procedures and medication optimization technologies in care transitions and disease management programs.

Copyright © 2012 Public Health Institute, Center for Technology and Aging.

1 Implement Policies & Procedures

Compliance involves the alignment of numerous internal and external variables, and relies on broad organizational understanding and agreement. Establishing reasonable and appropriate policies and procedures that guide organizational/workforce behavior is a critical first step toward compliance and, in turn, proper privacy and security.

With organizational policy as the foundation of an effective and secure system, the specific procedures of the program ensure its proper operation. As procedures will vary among programs, depending on the choice of technology to optimize medication use, this guide aims to provide direction and raise awareness of administrative safeguards that act to ensure ongoing security and privacy.

Understand current practices – An institutional audit may be a necessary and valuable first step in the development of a secure medication optimization program. A comprehensive audit will address risk analysis/assessment, gap analysis, remediation, contingency planning, and personnel policy.

Provide training to alleviate past and potential issues – Written compliance standards should be effectively communicated to staff members. All staff must understand how the compliance program works and their role in ensuring compliance. Training should also include operational computing practices for personnel, including emergency procedures for technology error, disaster and data recovery.

Ensure accountability and access control – Managerial oversight, incident reporting and personnel responsibility characterize a secure system. Topics of policies and procedures may include (among others):

- Security and HIPAA training for staff, including designation of responsibility for new training related to technology, policy and security development.
- Proper storage and maintenance of electronic data.
- Reporting and documentation of incidents or vulnerabilities to appropriate authorities with disciplinary capacities, such as the Advisory Committee.

Copyright © 2012 Public Health Institute, Center for Technology and Aging.

2 Integrate Technology Practices

Where patient-centered medication adherence and monitoring devices act as conduits of sensitive information, staff and procedures must adhere to strict privacy and security guidelines.

Privacy requirements and agreements – Formal agreements must be established within medication optimization programs. These agreements include research authorization and waivers, preparatory research reviews, data use agreements and accounts of research disclosures.

Patient privacy – Of utmost concern is the security and privacy of patient information. Agreements of informed consent, IRB requirements and contracts outlining patient rights and responsibilities are essential. These agreements work alongside an understanding of patient/caregiver abuse and procedures to ensure proper clinical practices and management of data.

Security elements – As patient data in a medication optimization program is transmitted in and through Web-based technology, the individual elements of the technology must be secure. To protect the confidentiality, integrity, and availability of data, security measures should include access controls, audit controls, confidentiality assurances, data integrity mechanisms, transmission control, and non-repudiation agreements.

3 Understand the Regulatory Landscape

Medication optimization programs may be subject to federal, state and local legislation, including that of the Joint Commission, HIPAA, Family and Educational Rights and Privacy Act, Americans with Disabilities Act, Rehabilitation Act, Gramm-Leach-Birley Act, and the Children's Online Privacy Protection Act.

While the specific demands of each of these policy measures will not be discussed in the toolkit, each is publicly available for individual examination.

Copyright © 2012 Public Health Institute, Center for Technology and Aging.