



Managing Information Privacy & Security in Healthcare

JCAHO/NCQA Recommendations for Protecting Personal Health Information: A Framework for Meeting the Challenges in a Managed Care Environment

By the Joint Commission on the Accreditation of Healthcare Organizations and
the National Committee on Quality Assurance

Developed with generous support from the W.K. Kellogg Foundation and
the Agency for Healthcare Policy and Research

Executive Summary

One of the touchstones of our health system is the deep trust that patients place in their providers. Patients entrust information to their doctors that they share with few other human beings. They know that this openness and honesty is essential to obtaining appropriate and effective Healthcare. Increasingly, however, some patients may pause before sharing certain information with their providers. They may wonder who in addition to their doctor will become privy to highly personal details. They are aware that some of their information must be shared with unknown individuals who handle reimbursement insurance and quality of care issues. However, they may wonder who else has access to their information, or how well is its privacy protected when transmitted electronically among these parties. To the extent that individuals needing healthcare withhold vital information because of these fears, potential complications could arise in relation to their treatment, and their very lives could be endangered.

Today's uncertainty about access to personal health information is sustained by the lack of consistent policies and practices for protecting the confidentiality of personal health data. Fair information practices that define individual rights and protections for other types of personal information, such as financial data, are not formally and uniformly applied to personal health information. Most stakeholders—provider organizations, practitioners, health plans, deliverers of specialty services (carve-out providers), claims administrators, and others—are generally committed to protecting the confidentiality of personal health information. In one form or another, all have policies and practices intended to protect confidential information. However, each group is left to its own best judgment as to the policies adopted and how they are applied when facing numerous demands for sharing sensitive information to accomplish routine management tasks related to oversight of care, reimbursement, utilization review, disease prevention, and resource management. Unfortunately, the framework or standards against which to evaluate these practices is often missing.

NCQA and JCAHO believe that concerns about confidentiality of personal health information seriously threaten the quality of healthcare. As accrediting organizations, NCQA and JCAHO believe that they can contribute to the development of a common framework to guide the protection of personal health information. Recognizing the societal importance of sharing personal health data in certain circumstances, this joint effort focused on the nature of the special concerns, problems, and strategies for addressing patient confidentiality issues in today's complex healthcare environment, where managed care organizations (MCOs), providers, employers, oversight organizations, regulators, and researchers require increased access to personal health information.

This paper presents an overview of the issues that were considered through the NCQA/JCAHO joint project, and identifies actions that can be taken to address the confidentiality of personal health information. This report is intended to inform legislators, policy makers, managed care plans, providers, and the public. Funding for this project was received from the W.K. Kellogg Foundation and AHCPH in the Department of Health and Human Services.

NCQA and JCAHO have incorporated requirements for the protection of patient information into their standards and practices for evaluating healthcare organizations. Today's accreditation standards address requirements for health organizations to: obtain patient consent for release of information; treat patient medical records as confidential; incorporate confidentiality requirements into contractual agreements with third parties; and inform patients of their rights regarding access to their medical record information. The accreditation review process also includes a contractual agreement that holds reviewers accountable for the confidential treatment of any patient data that is accessed during a review. As a result of the issues addressed and the recommendations developed in this report, NCQA and JCAHO will consider where these recommendations extend beyond current standards and practices and how they might influence modifications to their accreditation standards.

Throughout the healthcare system, among legislators, and across the general public there is consensus on the need to improve the protection of the confidentiality of personal health information. The recommendations presented in this report are a starting point to enable all participants to evaluate their policies and procedures and move forward with increased protections. Many of the actions described in this report can be implemented in a near-term timeframe and will significantly improve the protection of personal health information. The recommendations are divided into six major areas:

- Ensuring accountability
- Dealing with consent in an evolving healthcare delivery and financing system
- Educating about policies, practices, rights, and responsibilities
- Using technology as a solution
- Providing legislative support
- Guiding research

Recommendations

The recommendations present the positions of NCQA and JCAHO. They are derived from discussions during work sessions convened with numerous experts on this topic. However, they do not represent a consensus of the participants from those sessions, nor should they be attributed to any member or groups of members who participated in this project.

Ensuring Accountability

Managed Care Organizations (MCOs) should have clearly defined policies and procedures for dealing with confidentiality issues. The MCO policies and procedures should be built upon an understanding of stakeholders' views and values.

Accountability is enhanced by having focal points who are responsible for assessing compliance with policies and procedures, and addressing new requests for data—for example, a security officer and a data disclosure board.

MCOs should have a program of periodic audits to ensure compliance by staff and contractors with MCO policies and procedures. Audits should also include a determination of the accuracy of personally identifiable health data and should determine the rate, type, and source of errors.

All contracts, carve-outs, and carve-ins should be held to the same standard of accountability as the MCO. If an MCO shares patient data with these parties, such as for managed behavioral healthcare services, access to personally identifiable data for the patient's care by those services should be provided as needed. Accountability should be on (1) the MCO and (2) the contracted provider, so that protections are in place to allow access only by the appropriate caregiver.

Oversight organizations, including accrediting bodies, states, and federal agencies, should include terms in their contracts that describe their responsibility to maintain the confidentiality of any personally identifiable health information that they review. To the extent possible, these organizations should minimize their access to personally identifiable health information. Aggregated and/or de-identified data should be used whenever feasible.

MCOs must verify that personally identifiable health information shared with external organizations is used only for the purposes that were specified in the patient's consent, and that the external organization will comply with the MCO's policies.

There must not be any commercialization of patient identifiable information by MCOs or any organization handling patient data, without specific patient consent for this purpose.

Licensed, independent practitioners responsible for direct patient care should have access to all relevant personal health information on the patients they are treating.

As part of their assessment of managed care organizations competing for their business, employers should include requirements for the protection of personally identifiable health information. These criteria should also be incorporated into employer and other purchaser contracts with MCOs and applied in monitoring the performance of a managed care organization.

Employers should not have access to personally identifiable health information about their employees without consent or unless mandated by law. MCOs should not share personally identifiable health information with employers without consent. Self-insured employers should adopt technical and operational practices that protect personally identifiable health information from unauthorized access and meet the same standards of protection as required for MCOs.

Dealing with Consent in an Evolving Healthcare Delivery and Financing System

Use of an individual's personally identifiable health information for any purpose must be authorized by a

clear and specific consent provided by the patient unless the release of the information is required by law. Consents should be truly informed, specific, and voluntary. The language of the consent must be written in a manner that can be understood by the patient. Consents should specify the information to be shared, with whom, and for what purposes it will be used.

Providers and MCOs should have policies and procedures that can alert them to the need to obtain patient consent subsequent times.

Educating about Policies, Practices, Rights, and Responsibilities

MCOs should provide their members with a detailed understanding of what personally identifiable health information is maintained, how it is kept, how it is used, who has access to it for clinical, reimbursement, or for quality oversight purposes, and any releases of information that are required by law. MCOs should make their policies and procedures known at the time of marketing and enrollment and reinforce them at the time of care delivery. These efforts should be continuous and multi-pronged.

Practitioners and provider organizations should inform patients of their rights and responsibilities regarding the confidentiality of their information at the time of their initial encounter. This should be reaffirmed at other appropriate intervals, such as when there is a significant change in health status or in the use of their personal health information.

MCOs should inform their members of their rights to review and comment about their personal health information and to review transaction logs that record accesses and/or changes to their personally identifiable health information.

MCOs should routinely provide training to their employees and contracted providers on how to be sensitive to confidentiality concerns and how to comply with confidentiality policies.

Using Technology as a Solution

As MCOs acquire information systems, they should require capabilities that provide a high level of security and confidentiality protection, including encryption, detailed user access controls, transaction logs, and blinded files.

MCOs and providers should leverage the sophistication of technology to solve special privacy issues, such as restricted access. Existing technology can set levels of authorization for access to patient data according to the role the user plays in a patient's care.

MCOs should maintain and routinely analyze records of all accesses and/or modifications to personal health information. Modifications or changes to data should be disseminated in a timely way to all other legitimate users to ensure data accuracy. To the extent possible, this tracking should be incorporated into computerized systems.

Providing Legislative Support

Federal and state legislation should strive to provide consistency across jurisdictions and, at minimum, in all areas germane to patients' rights. States should have the flexibility to implement federal protections through regulations that address special considerations in their jurisdictions.

Legislation should provide equally high levels of confidentiality protection for all personally identifiable health information.

State and federal penalties for misuse that are meaningful deterrents should be designed and enacted in a way that is relevant to and reinforced by today's level of technical uses and capabilities.

Legislation should mandate that law enforcement officials must provide evidence of credible and compelling need for access to personally identifiable health information. Federal law should protect as confidential any quality improvement or risk-reduction information gathering done in response to a requirement by an accrediting or oversight body as part of its oversight activities.

In the absence of specific legislation, MCOs should have policies and procedures for determining when patient information should be turned over to law enforcement officials and conditions for doing so.

Guiding Research

When MCOs disclose personally identifiable health information to health service researchers, they should ensure that the intended research has had appropriate reviews and contains necessary controls to protect the confidentiality of the patient.

When MCOs share personally identifiable health information with researchers for record review or data linkages, anonymizing protections such as encryption and or de-identification techniques should be used whenever possible. Designated security and privacy personnel should protect any "keys" and these keys should be destroyed as soon as possible.

When MCOs agree to share identifiable information with researchers, they should include penalties in their contracts or collaborative agreements for any unauthorized use or disclosure of the data.

The research community, in collaboration with HHS, should develop principles to guide Institutional Review Boards (IRBs) when approving the use of personally identifiable health information. These principles should be used consistently across IRBs.