

# MODEL PRINCIPLES OF FAIR HEALTH INFORMATION PRACTICES

## Health Data Confidentiality

**Access:** Restrict internal and external access to automated medical records if access is not directly related to patient treatment and care.

**Release:** Prohibit release of identifiable or linkable medical record information to outside third parties (excluding insurance providers) without affirmative, informed patient consent.

**Secondary Use:** Limit the uses of identifiable or linkable medical record information for purposes unrelated to patient treatment and care and in the absence of patient consent.

## Database Management

**Integrity:** Develop policies and procedures to guard against inaccurate and outdated medical record information maintained in electronic format.

**System Design:** Build in patient privacy up-front when designing record-keeping systems that enhance efficiency, cost effectiveness and outcome evaluations.

**Authentication:** Prohibit record access to all but authorized health care providers; require password entry; institute audit trails to monitor access to electronic patient records.

## Patient Consent and Control

**Consent:** Require affirmative, informed patient consent for the release and sharing of medical record information (excluding insurance reimbursement and mandated reporting) that is not directly related to the patient's treatment and care.

**Control:** Re-examine the ethical imperative of meaningful and truly informed patient consent in light of growing demands for health data. Avoid the use (and overuse) of 'blanket consent forms' and the concept of 'implied consent.'

**Notice:** Require patient notice when identifiable or linkable patient information is released for (a) audits, (b) investigations of fraud and abuse, (c) law enforcement and (d) compliance with mandated government reporting.

**Patient Anonymity:** Use aggregate patient data for peer review, accreditation, survey and outcomes research as well as medical and pharmaceutical marketing.

**Surveys and Questionnaires:** Require informed patient consent for the release or re-release of identifiable or linkable patient information gathered from surveys, questionnaires or health screenings.

## Health Data Networks

**Data Collection:** Prohibit the consolidation and centralization of identifiable patient information unless the health data network is justified by an overwhelming public health need and governed by a signed legal agreement.

**Patient Identifiers:** Prohibit the use of the Social Security Number as a 'unique' patient identifier; utilize a neutral numbering system for sensitive health-related information.

**Data Linkage:** Restrict efforts to link personal patient information from remote sources, particularly if such efforts are used for prediction, profiling and outcomes research. Use aggregate data for research whenever possible; otherwise, obtain patient consent.

## Accountability

**Oversight:** Institute computer audit trails that document system activity, including the user's identity, date of access, time, location and information that was reviewed. Appoint a privacy officer as well as a patient rights advocate.

**Communications and Transmissions:** Caution against the use of unsecured e-mail and facsimiles to transmit sensitive health-related information. Warn employees against loose 'elevator talk,' public telephone conversations and open consultations.

**Enforcement:** Enact legislation and/or institute policies that create penalties for lapses of medical confidentiality and unauthorized release of patient information.

## Computer Security

**Prioritize Privacy:** Consider patient privacy a paramount policy objective when automating paper medical records, instituting telemedicine and introducing new and sophisticated technologies.

**Procedures:** Develop written policies and procedures requiring lock-outs, randomly selected passwords, screen savers, inactivity time-outs, audit trails and other barriers to guard against unauthorized or accidental breaches of medical confidentiality.

**Confidentiality Oaths:** Require employees to sign confidentiality statements annually and host periodic staff training in security and confidentiality procedures.

**Encryption:** Utilize pseudonyms, mathematical algorithms and encryption software to mask identifiable medical information that is transmitted to or shared with outside parties; otherwise, release only aggregate data.