

- D. **Electronic health information (such as electronic medical records)** is a computerized format of the health-care information in paper records that is used for the same range of purposes as paper records, namely to familiarize readers with the patient's status, to document care, to plan for discharge, to document the need for care, to assess the quality of care, to determine reimbursement rates, to justify reimbursement claims, to pursue clinical or epidemiological research, and to measure outcomes of the care process.
- E. **A firewall** is a computer positioned at a single focused point of entry for external users over unsecured public networks, such as the Internet, into an internal trusted network; firewalls can be configured to monitor and regulate messages passing into and out of the private network, or prevent particular programs from passing through.

VI. REFERENCES

- A. Information Management [00-01-10-30:00](#)
- B. *For the Record: Protecting Electronic Health Information, National Research Council, 1997* (from which sections of this policy have been taken verbatim).

VII. POLICY

A. General Principles:

1. Electronic health-care information has many advantages over paper records, including immediate availability to authorized individuals; clear organization; ready adaptability for analyses and research; legibility; and ability to provide alerts, suggestions, warnings, reminders, critical pathways and links to relevant literature. It will be the predominant form of health-care information at the University in the future. Properly implemented and managed, electronic health records have the potential to *increase* the security of health information and the privacy of patients over that in a paper-records environment.
2. Individuals have a fundamental right to control the dissemination and use of information about themselves, including health-care information. Individuals have the right to expect that their identifiable health information will not be disclosed without their express informed consent. Respect for patients' privacy is part of the ethical practice of the health-care professions.
3. The University is committed to providing appropriate safeguards for patient privacy and for confidential health-care information, consistent with available technology and with legitimate needs for accessibility of the information to authorized individuals for effective delivery of health care, for efficient functioning of the health-care delivery system (including audit and accreditation functions), for biomedical, behavioral, epidemiological and health services research, and for education.
4. Protection of health-care information depends on both technology and organizational measures to minimize potential abuse by authorized users, whether intentional or unintentional, and from outside attacks.
5. The technical and organizational security measures required to safeguard patient privacy and the confidentiality of health-care information must be balanced against: (a) costs (impediments to clinicians' access to information relevant to their decision-making; expense of purchase and of integration into the current system; costs of ongoing management, operations and maintenance; user frustrations with suboptimal interfaces and procedures; user time lost in satisfying security protections); (b) the need of

authorized users to access critical information in a timely manner so that provision of health care is not compromised; (c) the need of researchers and educators for information that will further knowledge; (d) and the desire of payers not to be defrauded.

6. The University requires compliance with all state and federal laws, rules and regulations governing the confidentiality of patient medical records in any medium, as well as with the guidelines established by organizations such as the JCAHO.
 7. Any individual who violates this policy or is responsible for unauthorized breaches of patient confidentiality shall be subject to discipline up to and including dismissal from the University as well as civil and criminal penalties. Sanctions shall be applied consistently to all violators regardless of job title or level in the organization.
- B. Security breaches, violations of policy, unauthorized access, audit-trail data or other system warnings about unusual or inappropriate activity, and identified weaknesses in security measures shall promptly be reported by the assigned data steward or confidentiality officer to the pertinent dean or vice president and to the Vice President for IST.
- C. Mechanisms for protecting health information include *technical measures* for improving computer and network security, and *organizational measures* for ensuring that health-care workers understand their responsibility to protect information and that processes are in place for detecting and reporting violations:
1. Technical Practices and Procedures: The University and its patient-care units shall adopt the following technical security practices:
 - a. *Individual authentication of users.* In order to establish individual accountability for actions on-line and to implement access controls based on individual needs, every individual shall have a unique identifier or log-on ID for use in logging into patient-care information systems. Individuals shall be informed that it is a violation of this policy to share identifiers with others. Passwords shall be changed no less frequently than every six (6) months. Names, English-language words and common acronyms shall not be used as passwords. Passwords should include letters, numbers and other characters. There shall be strict procedures set up at each patient-care unit for issuing and revoking identifiers.
 - b. *Access controls.* As soon as current technology at the University permits, each patient-care unit, patient-care center and faculty practice shall develop procedures to ensure that users can access and retrieve only that information for which they have a legitimate need to know.
 - c. *Audit trails.* Each patient-care unit shall maintain in retrievable and usable form audit trails that log accesses to patient information. The logs may include information such as the date and time of access, the information or record accessed, the user ID under which access occurred, and if possible the reason for the access.

Audit-trail information shall be kept in a safe place to prevent erasure or modification. Procedures shall be established for regularly reviewing and analyzing audit logs or a random sample thereof to detect inappropriate accesses. Audit trails should be used together with system-generated prompts or warning screens informing users of the sensitive content of patient records and reminding them about audit logs and sanctions for unauthorized access.

- d. *Physical security and disaster recovery.* IST and each patient-care unit shall: (1) limit unauthorized physical access to computer systems, displays, networks and health-care records; (2) position monitors and keyboards so they are not easily seen by anyone other than the user; (3) where appropriate, program workstations to display passworded screen savers if left idle for a specified period of time; (4) properly dispose of outdated equipment, tapes, disks, paper printouts and other media that contain confidential information; (5) establish plans for providing basic system functions and ensuring access to health-care records in the event of a natural emergency or mechanical or software failure by means such as redundant processing facilities, regular full-system back-ups and annual practice drills; (6) store back-up data in safe places or in encrypted form; and (7) ensure that contractors used to transport and store back-up tapes have adequate policies and procedures to protect the integrity and confidentiality of the information.
- e. *Protection of remote access points.* IST shall install and monitor a firewall and/or other forms of protection that provide strong centralized security to host machines that allow external public or insecure connections such as the Internet or dial-in telephone lines. Outside access shall be allowed only to those systems critical to outside users or for the conduct of University business. There shall be an additional secure authentication process (either encrypted or single-session passwords) for remote and mobile users, such as those using home or portable computers, *or* remote access shall be allowed only over dedicated lines.
- f. *Protection of external electronic communications.* In order to prevent interception by unauthorized individuals, all patient-identifiable information should be encrypted before transmission over open public networks such as the Internet, *or* such transmission should be only over secure dedicated lines. The inclusion of patient-identifiable information in unencrypted E-mail is forbidden.
- g. *Software discipline.* IST shall ensure the installation of virus-checking programs on all servers University-wide. The University shall maintain an inventory of all software on all workstations and servers. Vendor licensing agreements must be adhered to.
- h. *System assessment and technological awareness.* IST shall formally assess the security and vulnerabilities of the University's information systems on an ongoing basis, e.g., running "hacker scripts" and password "crackers" against the systems, and routinely using software protection tools such as virus-detection software and software checksum protection. IST shall also continuously appraise the University's system architecture, hardware and software technologies, and procedures to eliminate outdated components and practices.

IST shall aggressively stay current with standards and technologies for security management, and make recommendations to the University's patient-care units concerning the *future* implementation of new security practices that become state of the art, such as strong authentication practices, University-wide authentication systems, access validation, expanded audit trails, electronic authentication of records via electronic signatures, cryptographic technologies.

- 2. Organizational Practices: The University and its patient-care units shall adopt the following organizational security practices:
 - a. *Unit-specific security and confidentiality procedures.* Each patient-care unit, patient-care center and faculty practice shall develop explicit and clear confidentiality procedures governing both paper and electronic media that: (1) state the types of information considered confidential; (2) stipulate who may have access

to which elements of patient information for what purposes; (3) identify the people authorized to release the information and the procedures that must be followed to make a release; (4) identify the types of people authorized to receive information, under which circumstances, and when additional patient consent is required; (5) specify a method of disposal of paper records containing patient identifiers that ensures their complete destruction (i.e., shredding or bonded disposal); (6) enforce sanctions that will be applied for breaches of confidentiality and unauthorized access; and (7) set up training programs for staff, faculty and students in privacy, confidentiality and security. These policies and associated procedures should be reviewed annually and publicized regularly, preferably by senior management.

- b. *Unit security and confidentiality committees.* Each patient-care unit, center and faculty practice shall establish a broadly based committee or assign a person or office to develop, implement, monitor and maintain the unit-specific procedures for protecting patient privacy and ensuring the security of information systems. Similarly, responsibility shall be assigned for granting and removing access privileges to/from users of the unit's information system.
- c. *Education and training programs.* Each patient-care unit, patient-care center and faculty practice, in conjunction with IST, shall establish formal educational programs to ensure that all users of information systems receive the required training in professional responsibilities and personal accountability for security and confidentiality, in relevant security practices, and in existing confidentiality policies and proper procedures *before* being granted access to any health-information systems. Annual refresher courses should also be conducted with the participation of the medical staff leadership. Other educational tools, such as in-service sessions, grand rounds, continuing medical education, selective use of one-on-one or small-group training for physicians, videos, pamphlets, posted reminders, on-line screens, memos and newsletters should be considered. System users requiring training include full-time, part-time, temporary and newly transferred employees, admitting and referring physicians, contractors, vendors, housestaff, students, volunteers, and outcomes or epidemiological researchers.

Log-in screens should be developed that remind users that health-care information is limited to legitimate health-care or research purposes, that misuse of health-care information is a violation of University policy and can lead to sanctions, and that audit logs record all user activities.

- d. *User confidentiality agreements.* Any individual (employee, student, volunteer, contract worker, vendor or other non-employee) accessing patient-information systems must sign a form stating that she or he has read, received a copy of, understood and will comply with this University policy and the patient-care unit's procedures. This form should be signed *prior to* access being given and retained in the pertinent department. The unit's data steward or confidentiality officer shall ensure the signing of these agreements and keep the forms on file.
- e. *Informing patients.* Each patient-care unit, patient-care center and faculty practice shall develop means to inform patients of the existence of electronic health records, to describe health-data flows within the unit and with external organizations, to describe the policies and procedures in place to protect patient privacy, to request additional patient authorizations for other proposed uses of their health information, and to inform patients of their rights of access to their health records. This information should list the types of organizations and individuals to whom identifiable and unidentifiable information is commonly released (such as insurers, managed care companies, responsible researchers with appropriate IRB approval and patient consent, certain government agencies, courts, accreditation and

oversight bodies, authorized social-welfare agencies, etc.). Methods to accomplish this include disclosure authorization forms separate from other consent forms such as those for medical care or research. The time period for which authorizations are valid should be indicated.

- f. *Patient access to audit logs.* The University's health-care units, centers and faculty practices should give patients the right to request and review audits of all accesses to their health records, as well as the right to review the contents of their health records and annotate or supplement information they believe to be inaccurate, incorrect or incomplete (without removing any information). Patients' primary care physicians also have the right to review audit logs of their patients' health records.

By Direction of the President:

Vice President for Information Services & Technology

Associate Vice President for Academic Affairs