Privacy has many aspects. Among them is the ability to control personal information and the right to keep it from misuse.

Security measures attempt to protect computer systems, including information, from harm and abuse; the threats may stem from many sources including natural disaster, human error, or crime including the spreading of viruses.

Protection may take the form of anything from professional and business codes of conduct, to laws, to restricting access to the computer.

Computer technology has led to new forms of crime. Crimes involving computers can be crimes using computers and/or crimes against computer systems.

- **Software piracy**
- **Theft of services**
- **Theft of information**
- **Fraud**
- **Spread of viruses**
- **Identity theft**
- **Other threats to computer systems**
  - Spyware is software that can be installed without the user’s knowledge to track their actions on a computer.
  - Adware may display unwanted pop-up advertisements displayed on your monitor; it may be related to you the sites you search on the Web or even the content of your e-mail.
  - A fraudulent dialer can connect the user with numbers without the user’s knowledge.
  - Keylogging can be used by anyone to track anyone else’s keystrokes.
  - Malware includes different forms of malicious hardware, software, and firmware.

Security measures

- **Internal codes of conduct (self-regulation)**
- **Audit trails**
- **Encryption**
- **Laws**
  - Fair Credit Reporting Act
  - Federal Privacy Act
  - Health Information Portability and Accountability Act
  - Online Privacy Protection Act
- **Restricting access**
  - Personal identification numbers (PINs)
• Biometrics—fingerprinting, retina or iris scan, biometric keyboards, lip prints, facial thermography, body odor sensors, voice recognition, DNA

• RFID tags
• Backscatter X-ray machines to search air travelers (also known as the virtual strip search)
• Firewalls

• Privacy

• Computers and networks allow personal information to be centralized and gathered easily.
• As an employee
  • E-mail (at work) is not private.
  • Background checks
• Real ID Act of 2005 “directly imposes prescriptive federal driver’s license standards” by the federal government on the states
  • Requires every American to have an electronic identification card
  • State Departments of Motor Vehicles (DMV) must share all the information in their databases with all other state DMV’s databases. This creates a huge database.
  • A new threat to personal privacy may come from implanted RFID tags (Verichips).

• Databases—an electronic database is an organized collection of data that is easy to access, manipulate, search, and sort.
• Government databases
  • Only the federal government has some restrictions on how it uses information although this may be weakened by the USA Patriot Act and the Homeland Security Act.
    • These acts give law enforcement greater power to demand information and limit Congressional oversight.
  • Homeland Security is now sharing data with the Centers for Disease Control (CDC) in violation of its own agreement with the European Union (EU).
    • Some states and municipalities are putting all their records online.
    • The Real ID Act of 2005 will (if successful) establish a distributed database containing every person in the United States.
• Private databases—private organizations keep computerized databases of employees and potential customers. Hospitals keep records of patients.
  • Medical Information Bureau is composed of 650 insurance companies. Its database contains health histories of 15 million people. It is exempt from HIPAA.
  • Credit bureaus—credit history and credit report. Your credit report is used as a basis for granting or denying you a credit card, or mortgage, or car loan.
  • Data warehouses exist for the sole purpose of collecting and selling personal information. They sell information to credit bureaus and to employers for background checks.
• Databases and the Internet—computerized files are kept on networks; many of these networks are linked to the Internet. The information includes highly personal data such as Social Security numbers, dates of birth, mother’s maiden name, and unlisted phone numbers.

Privacy, security, and health care
• Health Insurance Portability and Accountability Act (HIPAA) of 1996
  • By encouraging the use of the electronic medical record and facilitating the sharing of medical records among health care providers, it can assure continuity of care and thus save lives.
  • However, the more easily your records are available, the less secure they are. Medical information can be used against you.
  • All patients have the right to see their medical records and request changes; patients will have some knowledge of the use of their medical records and must be notified in writing of their providers’ privacy policy.
  • The regulations cover “[a]ll medical records and other individually identifiable health information used or disclosed by a covered entity in any form, whether electronically, on paper, or orally. . . .”
  • In 2006, enforcement of HIPAA is lax.
  • Under both HIPAA and the Patriot Act, there are many circumstances that allow police access to your medical records without a warrant.
• HIPAA requires that you be informed in a general way how your records may be used without consent. However, you do not have to be notified of any specific sharing of your information, and further the USA Patriot Act does not allow you to be told.
• HIPAA requires that e-mail be secured by either by using encryption or controlling access. HIPAA specifically discusses privacy issues of telemedicine, including the presence of nonmedical personnel (e.g., camera people and other technicians) and the fact that the more stringent privacy protection (federal or state) has precedence.

• As research focuses on genetics and an individual’s genetic probability of developing certain diseases, privacy issues arise.

• The problems of protecting private medical information may multiply if all medical and health records are digitized and put online under a national system proposed by the Health Information Technology Decade. Security breaches are common.