Confidentiality, Privacy and Security

Privacy

- The desire of a person to control the disclosure of personal health information

Confidentiality

- The ability of a person to control release of personal health information to a care provider or information custodian under an agreement that limits further release of that information

Security

- Protection of privacy and confidentiality through policies, procedures and safeguards.

Why do they matter?

- Ethically, privacy and confidentiality are considered to be rights (in our culture)
- Information revealed may result in harm to interests of the individual
- The provision of those rights tends to ensure that the information is accurate and complete
- Accurate and complete information from individuals benefits society in limiting spread of diseases to society (i.e. HIV)

Why do they matter?

- The preservation of confidentiality assists research which in turn assists patients

Users of health information

- Patient
  - Historical information for current and future care
  - Insurance claims
- MD's
  - Patient's medical needs
  - Documentation
  - Interface with other providers
  - Billing

Users

- Health insurance company
  - Claims processing
  - Approve consultation requests
- Laboratory
  - Process specimens
  - Results reporting
  - Billing

Users

- Pharmacy
  - Fill prescription
  - Billing
- Hospital
  - Care provision
  - Record of services
  - Billing
  - Vital statistics
  - Regulatory agencies

Users

- State bureau
  - Birth statistics
  - Epidemiology
- Accrediting organization
  - Hospital review
- Employer
  - Request claims data
  - Review claims for $ reduction
  - Benefits package adjustments

Users

- Life insurance companies
  - Process applications
  - Process claims
  - Risk assessment
- Medical information bureau
  - Fraud reduction for life insurance companies
- Managed care company
  - Process claims
  - Evaluate MD's

Users

- Lawyers
  - Adherence to standard of practice
  - Malpractice claims
- Researcher
  - Evaluate research program

Security

- Availability
- Accountability
- Perimeter definition
- Rule-limited access
- Comprehensibility and control

Privacy solutions

- Forbid the collection of data that might be misused
- Allow the collection of health information within a structure, but with rules and penalties for violation pertaining to collecting *organizations*
- Generate policies to which *individual* information handlers must adhere

Security controls

- Management controls
  - Program management/risk management
- Operational controls
  - Operated by people
- Technical controls
  - Operated by the computer system

Management controls

- Establishment of key security policies, i.e. policies pertaining to remote access
  - Program policy
    - Definition, scope, roles and responsibilities of the computer security program
  - Issue specific policy
    - Example: Y2K
  - System specific policy
    - Who can access what functions where

Core security policies

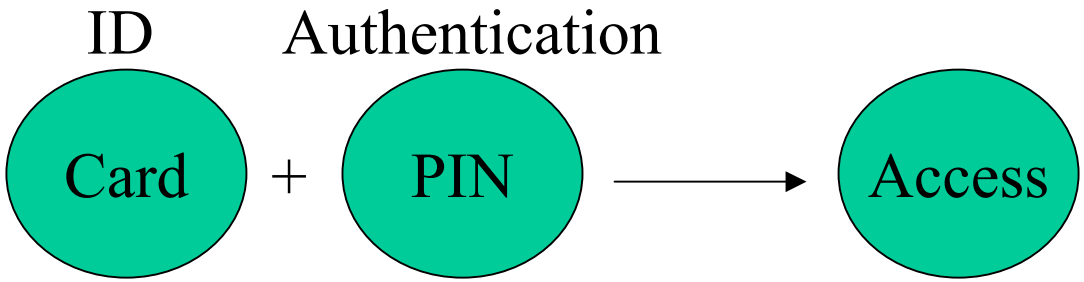
- Confidentiality
- Email
- System access
- Virus protection
- Internet/intranet use
- Remote access
- Software code of ethics
- Backup and recovery
- Security training and awareness

Biometrics

- The scientific discipline of measuring relevant attributes of living individuals or populations to identify active properties or unique characteristics
  - Can be used to evaluate changes over time for medical monitoring or diagnosis
  - Can be used for security

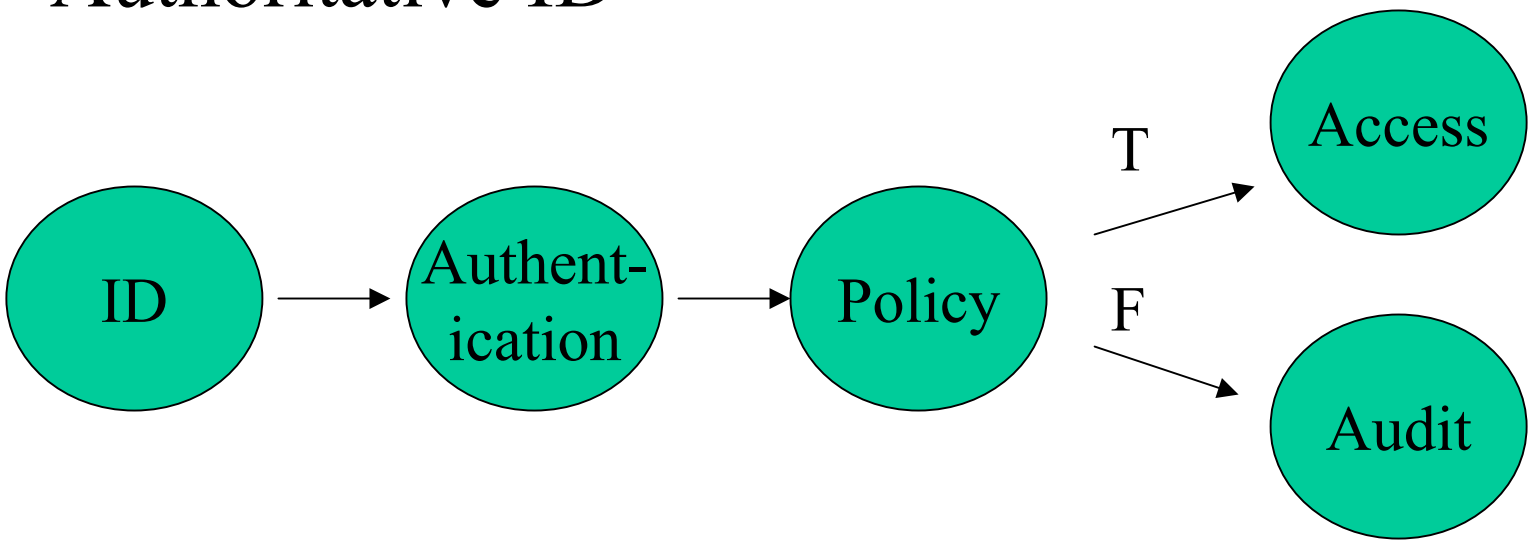
Approaches to identification

- Token based simple security
  - House key, security card, transponder
- Knowledge based
  - SSN, password, PIN
- Two-factor
  - Card + PIN



Approaches to identification

- Authoritative ID



Identification

- Certain and unambiguous
  - Deterministic
- Certain with small probability of error
  - Probabilistic
- Uncertain and ambiguous
- Biometric schemes are probabilistic

Probabilistic

- False acceptance rate (type I error)
  - Percentage of unauthorized attempts that will be accepted
  - Also relevant for medical studies
- False rejection rate (type II error)
  - Percentage of authorized attempts that will be rejected
  - Also relevant for medical studies
- Equal error rate
  - Intersection of the lowest FAR and FRR

Biometric ID

- Acquire the biometric ID
  - How do you ensure that you got the right guy
- Localize the attribute
  - Eliminate noise
  - Develop a template (reduced data set)
- Check for duplicates

Biometric applications

- Identification
  - Search the database to find out who the unknown is
  - Check entire file
- Authentication
  - Verify that the person is who he says he is
  - Check his file and match

Biometric identifiers

- Should be universal attribute
- Consistent – shouldn't change over time
- Unique
- Permanent
- Inimitable (voice can be separated from the individual)
- Collectible – easy to gather the attribute
- Tamper resistant
- (Cheaply) comparable - template

Biometric technologies

- Fingerprint
  - Automated fingerprint ID systems (law enforcement)
  - Fingerprint recognition – derives template form features for ID
  - Validating temp and /or pulse
  - Optical vs. solid state (capacitance)
  - Low FAR and FRR

Fingerprint

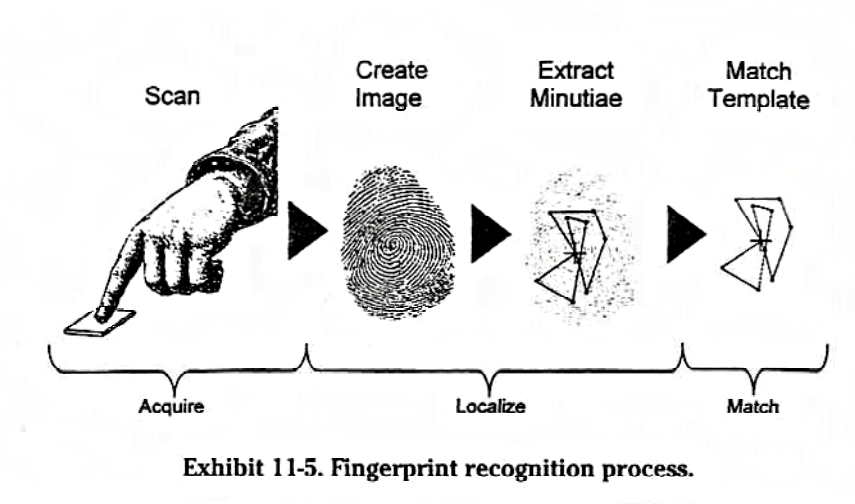


Exhibit 11-5. Fingerprint recognition process.

Hand geometry

- Dimensions of fingers and location of joints unique
- Low FAR FRR

Retinal scan

- Very reliable
- More expensive than hand or fingerprint
- Extremely low FAR FRR

Retinal scan

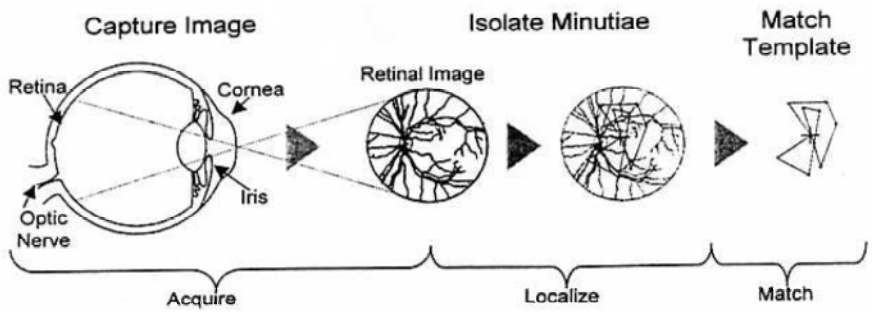


Exhibit 11-6. Retinal recognition process.

Voice recognition

- Automatic speaker verification (ASV) vs. automatic speaker identification (ASI)
  - ASV = authentication in a two-factor scheme
  - ASI = who is speaker
  - Feature extraction and matching
  - Problems with disease/aging etc.

Iris scanning

- Less invasive than retinal scanning
- Technically challenging balancing optics, ambient light etc.
- Can be verified (live subject) by iris response to light

Face recognition/thermography

- Facial architecture and heat signature
- Relatively high FAR/FRR
- Useful in two factor scenarios

Hand vein

- Infrared scanning of the architecture of the hand vessels

Signature

- Architecture of the signature
- Dynamics of the signature (pressure and velocity)

	Attribute								System			Suitability	
	Universal	Consistent	Unique	Permanent	Inimitable	Collectible	Tamper Resistant	Comparable	Performance	Authoritative	Reliability	Relative Cost	Acceptability
Fingerprint	◐	◐	●	●	●	●	●	●	●	◐	●	◐	◐
Hand Geometry	◐	●	●	●	●	●	◐	●	●	◐	●	◐	◐
Retinal Scan	●	●	●	●	●	◐	●	●	●	●	●	●	○
Voice Print	◐	●	◐	●	◐	●	◐	◐	○	○	○	◐	○
Iris	●	●	●	●	●	●	●	●	●	●	●	◐	◐
Hand Vein	●	●	◐	●	●	●	●	◐	◐	◐	●	◐	◐
Signature	○	○	○	○	○	◐	○	◐	○	○	○	◐	◐
Face Recognition	●	◐	◐	◐	○	●	◐	◐	◐	◐	◐	●	◐
Thermogram	●	◐	◐	◐	◐	●	●	◐	◐	◐	◐	●	◐

High = ●

Medium = ◐

Low = ○

Exhibit 11-7. Comparison of representative technologies.

Biometric identification issues

- Privacy, anonymity
- Legal issues not defined

Security: availability

- Ensures that accurate, up-to-date information is available when needed at appropriate places

Security: accountability

- Ensures that users are responsible for their access to and use of information based on a documented need and right to know

Security: perimeter definition

- Allows the system to control the boundaries of trusted access to an information system both physically and logically

Security: rule-limited access

- Enables access for personnel to only that information essential to the performance of their jobs and limits the real or perceived temptation to access information beyond a legitimate need

Security: comprehensibility and control

- Ensures that record owners, data stewards and patients can understand and have effective control over appropriate aspects of information confidentiality and access

Availability

- Backups with local and off-site copies of the data
- Secure housing and power sources for CPU even during disasters (when system availability may be crucial)
- Virus protection

Accountability

- Audit trails and warnings
- User
  - Authentication – unique ID process
  - Authorization – to perform set of actions, i.e. access only their own patients

Perimeter definition

- System knows users and how they are using the system
  - Define the boundaries of the system (i.e. within the firewall) Princeton-Penn-HUP
  - How do you permit/monitor off-site access
  - Modems?
- Tools
  - Cryptographic authentication

Perimeter definition

- Public key-private key
  - Encryption
    - Privacy and confidentiality
  - Digital signatures
    - Prescription signature
  - Content validation
    - Message hasn't been messed with
  - Nonrepudiation
    - "I didn't say that"

Role limited access

- Spheres of access
  - Patient list: patients one has a role in the care of
  - Content specific: billing clerk/billing info
  - Relevant data: researcher on heart disease shouldn't be able to learn about HIV status

Taxonomy of organizational threats

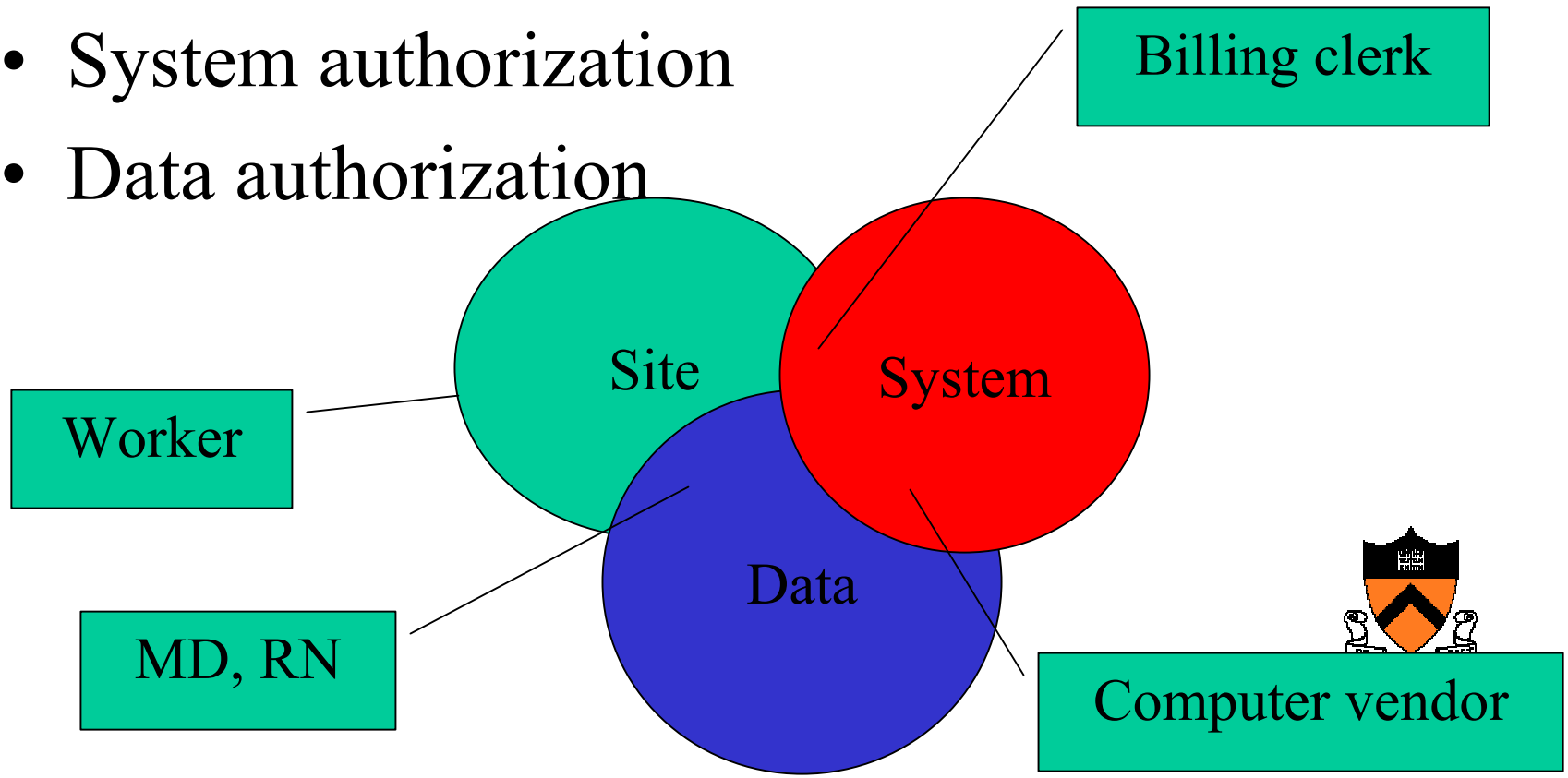
- Motive
  - Health records have economic value to insurers, employers, journalists, enemy states etc.
  - Curiosity about the health status of friends, romantic interests, coworkers or celebrities
  - Clandestine observation of employees (GE)
  - Desire to gain advantage in contentious situations (divorce)

Resources

- Attackers may range from
  - Individuals
  - Small group (e.g. law firm)
  - Large group (e.g. insurer, employer)
  - Intelligence agency
  - Organized crime

Initial access

- Site access
- System authorization
- Data authorization



Technical capability

- Aspiring attacker (limited skills)
  - Research target
  - Masquerade as an employee
  - Guess password
  - Dumpster diving
  - Become temporary employee

Technical capability

- Script runner
  - Acquire software from web-sites for automated attacks
- Accomplished attacker
  - Able to use scripted or unscripted (ad-hoc) attacks

Levels of threat

- Threat 1
  - Insiders who make “innocent” mistakes and cause accidental disclosure
  - Elevator discussion, info left on screen, chart left in hallway etc.
- Threat 2
  - Insiders who abuse their privileges

Threat

- Threat 3
  - Insiders who access information inappropriately for spite or profit
  - London Times reported that anyone's electronic record could be obtained for $300
- Threat 4
  - Unauthorized physical intruder
  - Fake labcoat

Threats

- Threat 5
  - Vengeful employees or outsiders bent on destruction or degradation, e.g. deletion, system damage, DOS attacks
  - Latent problem

Countering threats

- Deterrence
  - Create sanctions
  - Depends on identification of bad actors
- Imposition of obstacles
  - Firewalls
  - Access controls
  - Costs, decreased efficiency, impediments to appropriate access

Countermeasures

Type	System	Data	Site	Threat	Counter
1	Y	Y	Y	Mistake	Org and technical measures
2	Y	Y	N/A	Improper use of access privileges	Authentication and auditing
3	Y	N	N/A	Unauthorized for spite of money	Authentication and auditing
4	Y	N	Y	Unauthorized physical intrusion	Physical security and access control
5	Y	N	N	Technical breakin	Authentication, access and crypto

Counter threat 1

- Behavioral code
- Screen savers, automated logout
- ? Patient pseudonyms

Counter threat 2

- Deterrence
- Sanctions
- Audit
- Encryption (user must obtain access keys)

Counter threat 3

- Audit trails
- Sanctions appropriate to crime

Counter threat 4

- Deterrence
- Strong technical measures (surveillance tapes)
- Strong identification and authentication measures

Counter threat 5

- Obstacles
- Firewalls

Issues with countermeasures

- Internet interface
- Legal and national jurisdiction
- Best balance is relatively free internal environment with strong boundaries
  - Requires strong ID/auth

Recommendations

- Individual user ID and authentication
  - Automated logout
  - Password discipline
- Access controls
  - Role limited
  - Role definitions
    - Cardiologist vs. MD
- Audit trails

Recommendations

- Physical security and disaster recovery
  - Location of terminals
  - Handling of paper printouts
- Remote access points
  - VPN's
  - Encrypted passwords
  - Dial-ins

Recommendations

- External communications
  - Encrypt all patient related data over publicly available networks
- Software discipline
  - Virus checking programs
- System assessment
  - Run scripted attacks against one's own syste

Recommendations

- Develop security and confidentiality policies
  - Publish
  - Committees
  - ISO's
  - Sanctions
- Patient access to audit logs
  - Who saw my record and why

Future recommendations

- Strong authentication
  - Token based authentication (two factor)
- Enterprise wide authentication
  - One-time login to authorized systems
- Access validation
  - Masking
- Expanded audit trails
- Electronic signatures

Universal patient identifier

- Methodology should have an explicit framework specifying linkages that violate patient privacy
- Facilitate the identification of parties that make improper linkages
- Unidirectional – should facilitate helpful linkages of health records but prevents identification of patient from health records or the identifier