Patient Identification: Biometric or Botched

Raymond D. Aller, M.D.,
FASCP, FCAP, FACMI, LFHIMSS, BCI(ABP)
Clinical Professor of Pathology
University of Southern California

Pathology Informatics 2016
23 May 2016
Pittsburgh, PA

Notice of Faculty Disclosure

In accordance with ACCME guidelines, any individual in a position to influence and/or control the content of this ASCP CME activity has disclosed all relevant financial relationships within the past 12 months with commercial interests that provide products and/or services related to the content of this CME activity.

The individual below has responded that he/she has no relevant financial relationship(s) with commercial interest(s) to disclose:

Raymond Aller, MD

Agenda

- Overview of a patient identification ecosystem
- Text-based matching: unsafe, inaccurate, costly, and labor-intensive
- A better choice - identifying patients by who they are, or how they act,
  - not what they know or what they have
- Commonly used biometric identification technologies
- Clinical experience with various methodologies

Learning objectives

1. Describe the shortcomings and liabilities of text-based patient identification and matching

2. Categorize difficulties encountered when asking patients to identify themselves based on what they know, or what they have (ID card)

3. Contrast several of the technologies available to identify who a patient IS (e.g., fingerprint), or how they behave (signature tempo) and differentiate the diverse clinical situations for which different tools are best suited

4. Discuss the three phases of positive patient identification, and compare the technical and sociological aspects of the most commonly used biometric tools, to have the best chance of achieving maximum acceptance and interoperability

5. Apply beyond a departmental perspective to work with other parts of the healthcare enterprise (patent registration, nursing, I/T) to implement all three phases of positive patient identification in one's own organization

First things first – who is the patient?

»

- Well … of ***course*** we know …..but do we?
- In a few short months of oncology treatment, in an exclusive tertiary medical center, a single patient encountered two instances of potentially disastrous misidentification:
  - We're going to treat this tumor (but it was someone else's)
  - We're set up to irradiate your hip and shoulder … but … you don't have shoulder pain ??
- If it is this bad in private centers … what is the situation in *safety-ne*t institutions?

- It is NOT OK to diagnose or treat patients without FIRST knowing who they are

Of course we are treating the right patient!

»

- Our staff is very careful!
- We double-check all our work
- We check two identifiers (the JCAHO fallacy)
- We don't know about misidentifications – so they must not happen
  - One company advertises "error-free patient identification" – but there has been no measurement of the error rate
- A CMIO – "only a minority of hospitals are positively identifying patients for transfusion – or securely matching blood transfusions – therefore it is just a "nice to have" and I decided not to purchase that feature"

Consequences of failing to ID patients accurately

»

- Medical – treatment based on someone else's results
  - Incorrect/incompatible transfusions
  - Incorrect procedures
  - Delayed/wrong therapies
  - Misplaced diagnosis: malignancy, HIV
  - in one hospital, 3 years running -
  - total prostatectomy, benign
  - HIV+ reported to public health
  - Longer length of stay, higher costs
  - Breach of patient-provider relationship/trust
  - Adverse, sometimes fatal outcomes
- An abundance of legal and liability issues
- A public relations disaster

"Cost justification" of patient ID: an oxymoron »

- Do we ask that seat belts or brakes be cost-justified when we buy a car?
- Consider the legal, moral, and public relations consequences of
  - Diagnosing the wrong specimen
  - Treating the wrong patient
  - Taking action based on wrong blood in tube
- It's inexcusable to sell a car without brakes or seat belts
  - Why do we think it's OK to use crude manual "identification" tools, that permit gross misidentification?

Is this your hospital's view of patient ID?

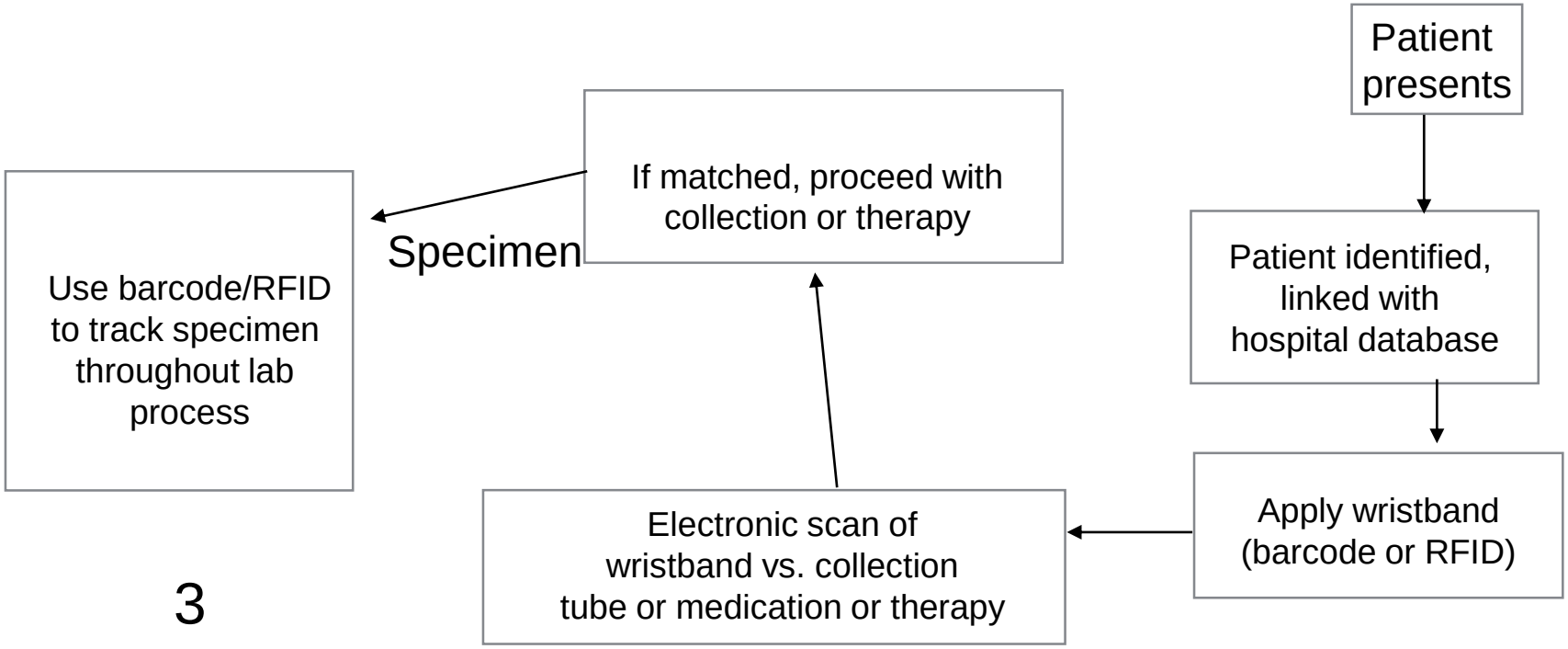
»

Three phases/stages of secure identification

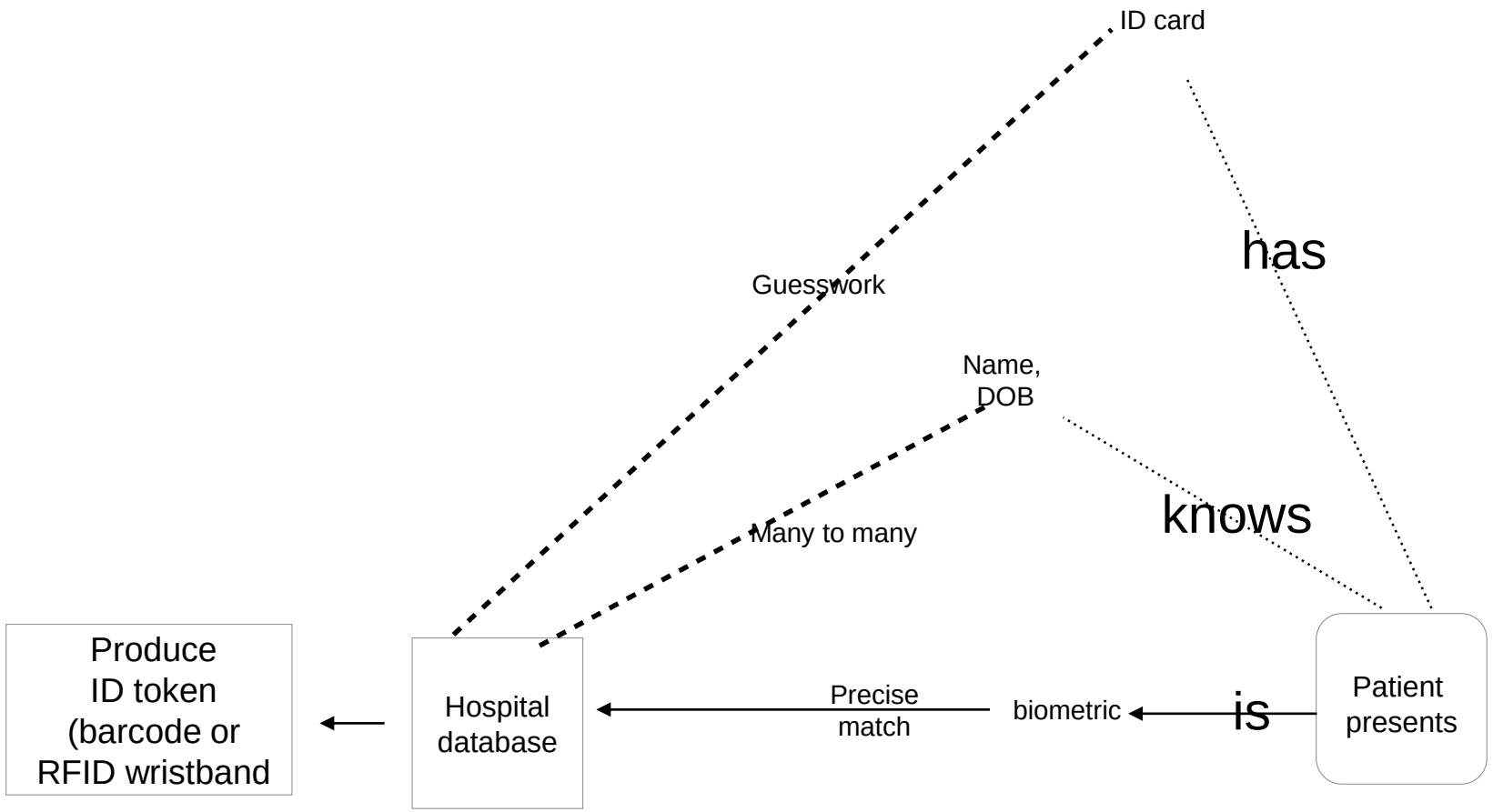
»

- 1. Secure registration
  - Establishing a record – linkage of that patient – biologically – to a logical entry within your information system
  - Connecting to previous visits by that patient (with identical biometrics)
  - Securely applying a token (barcode or RFID wristband)
- 2. Assured linkage of patient identification to every diagnostic specimen and therapeutic event
- 3. Unbroken robust tracking of specimens from collection through result
  - Clinical lab, anatomic pathology, etc.

Chain of identification - summary



Chain of identification - part 1



An obsolete approach to identifying patients – the illusion of text-based ID

Registration, with the patient in front of you

1. Ask name, data of birth
    A. The premise – similar name – but thousands of people share these identifiers
2. Have you been here before?
    A. Was I conscious? (am I now?)
    B. Was it to a different building?
    C. How long ago?
    D. Isn't medical care something we try to forget?

The illusion of text-based ID - part 2

3. Additional text identifiers
   - Address
   - Third cousin's favorite color
4. Hospital ID card – the sickest patient probably forgot to bring it – or the family picked up the sister's card on the way to the ED
5. Driver's license
   - Many people look like other's pictures
   - How many 19 year olds have a (fairly convincing) fake ID
   - How many others maintain a 12-year-old picture because it looks better?

Higher risk situations

»

- Siblings, twins – especially if simultaneous appointments
- Unconscious patient – and their wallet (even if it has not been stolen) likely won't have all the secondary and tertiary keys needed by text-based identifier systems
- Common names
  - But what is a common name?
  - In some localities, Shisnetski may be more common than Smith
  - In the United States, there are 50,000 Maria Garcias – how is the patient to know which one she is?
- Look alike, sound alike names
  - Ann E vs Annie
  - Nicknames

An obsolete approach to linking patients – the master patient index

»

- A large collection of patients in a database
- Uses as many fields as possible to test for linkage between patients
  - Fancier and fancier matching algorithms
  - Even greater illusion
  - Depending on local demographics, these may function decently – but is giving inappropriate treatment to even 1% of your patients acceptable?
- A large Midwestern teaching hospital –
  - We don’t have a problem with patient identification – it’s not on our radar screen (meaning - we have never measured it)
- Weakness of the MPI – depends on data supplied by the patient (what they know) – which is not unique
- In 2016, the MPI is an obsolete and dangerous concept.

Sometimes the patient *wants* to be mistaken for somebody else

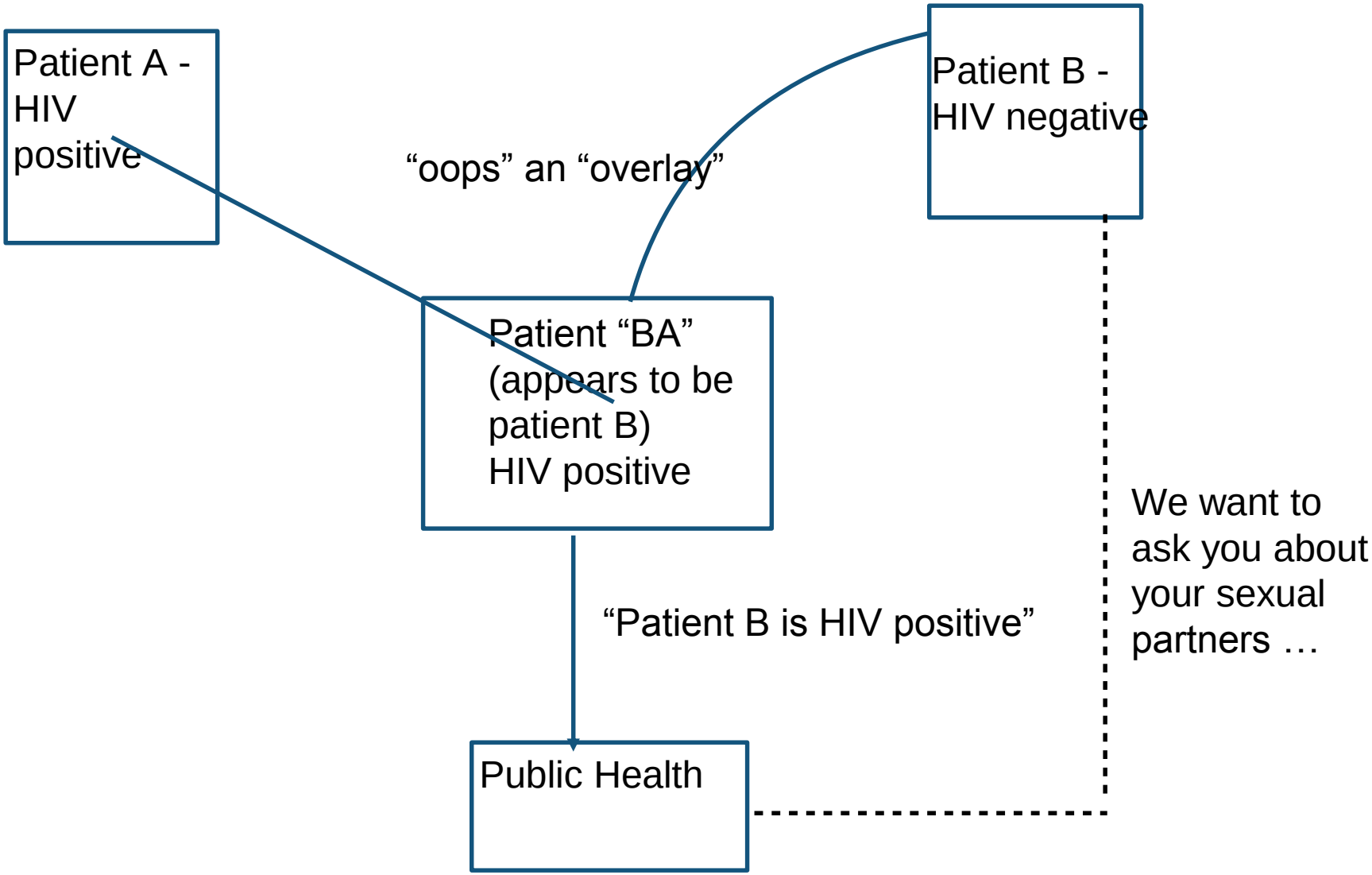
- I'm using my brother's Medicaid card of driver's license because I don't have health coverage
- Outright fraud – stealing from insurance, and from the hospital
- Medical identity theft – Sue has great coverage, so I'm pretending to be her to get my knee replaced
- Unfortunately for me, my blood type is different – but luckily, most blood banks have quadruple checking to prevent a disaster
- How many of our hospitals have a mechanism for tracking how many patients are admitted and treated under an assumed or stolen name?
- We cannot assert that it is "not a problem" if we don't measure it!!

The merge: consequence of patient misidentification

»

- Merge miasma – the necessity to merge different patient records, without knowing if they are really the same person
- Oops … we have an “overlay” … then we must un-merge, if we can
- Merging – a dangerous and misguided activity
- One urban hospital spent millions of dollars and over a year on a massive merge – and then a lot more on cleaning up the mess they had created
- On an ongoing, yearly basis, they continue to spend over $500,000 in personnel costs alone, to continue doing merges
- Three years later, that same hospital accidentally merged 1600 patients – and spent close to $100,000 straightening out the mess – including trying to explain to local Public Health that some of the HIV+ results they had been sent might have belonged to a different patient.

Merge mayhem



How (un)reliable is matching on the name and date of birth?

»

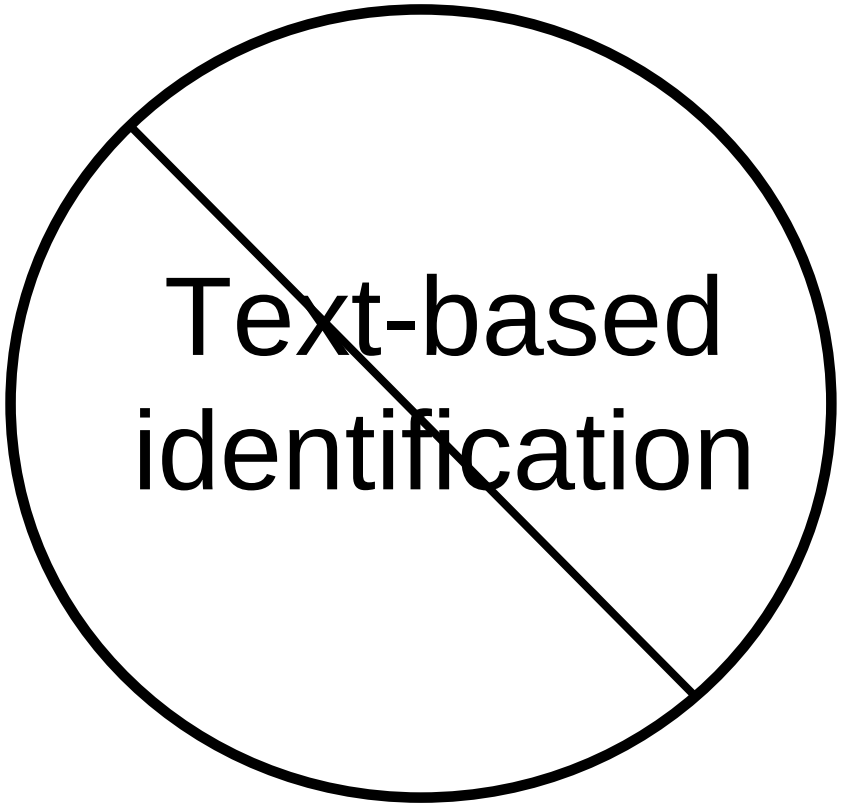
- Case study: Harris County Hospital 'District
  - Number of patients in the HCHD database – 3,428,925
  - Number of times when 2 or more patients share the same last and first names – 249,213
  - Number of times when five or more patients share the same last and first names – 76,354
  - Number of times when 2 or more patients share the same last and first names, and date of birth 69,807
  - Number of patients named Maria Garcia 2488
  - Number of Maria Garcia's with the same DOB 231
- Nationally
  - Duplicate records account for 5-15% of all patient records (source: ONC white papers) and cost the average hospital $500k to $2.5m every few years

Common names ….

»

- Hispanic women often use multiple last names: a colleague tells me that, on average, the women in his clinic use four last names - in varying order
- In some parts of the world (e.g., Southern India), people have only ONE name
- 50,000 people in the US share the name Maria Garcia (source: whitepages.com)
- It is a dangerous illusion that a text- based system will be able to reliably sort this out, to determine which ONE in 50,000 is sitting in front of us ….

»


Text-based
identification

Instead, we should seek data that will allow us to reliably recognize the patient the next time they appear

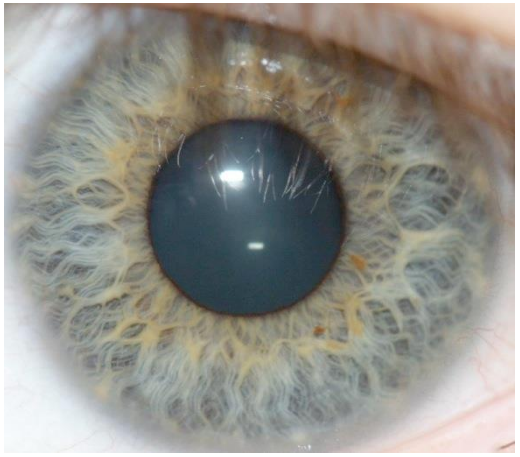
- A biometric identifier – a body characteristic that allows one to uniquely identify an individual
- Typically can be distinguished at a 1 in a million or better accuracy
- There are dozens of unique, or relatively unique, characteristics of the body – who they are (or how they act) not what they know
- A given biometric can be measured by a number of different tools, with varying degrees of precision
- So far, there are a few that have proven most useful. Each of these is useful in somewhat different circumstances
- Each has characteristics, strengths, and weaknesses
- Over 350 hospitals and other healthcare organizations (e.g., regional blood centers) around the US have already adopted biometrics for patient registration

Biometric identifiers – dozens of possibilities

- Those most commonly used in healthcare
  - Iris pattern
  - Palm vein
  - Fingerprint

- Also interesting
  - Signature/signature tempo
  - Finger vein
  - Hand configuration (US immigration, 1998)
  - Face recognition (NOT the same as “Picture ID”)
    - INS - Global Entry
  - Voice
  - Cardiac rhythm

Biometric Tools



These, and several others

Iris Scanning

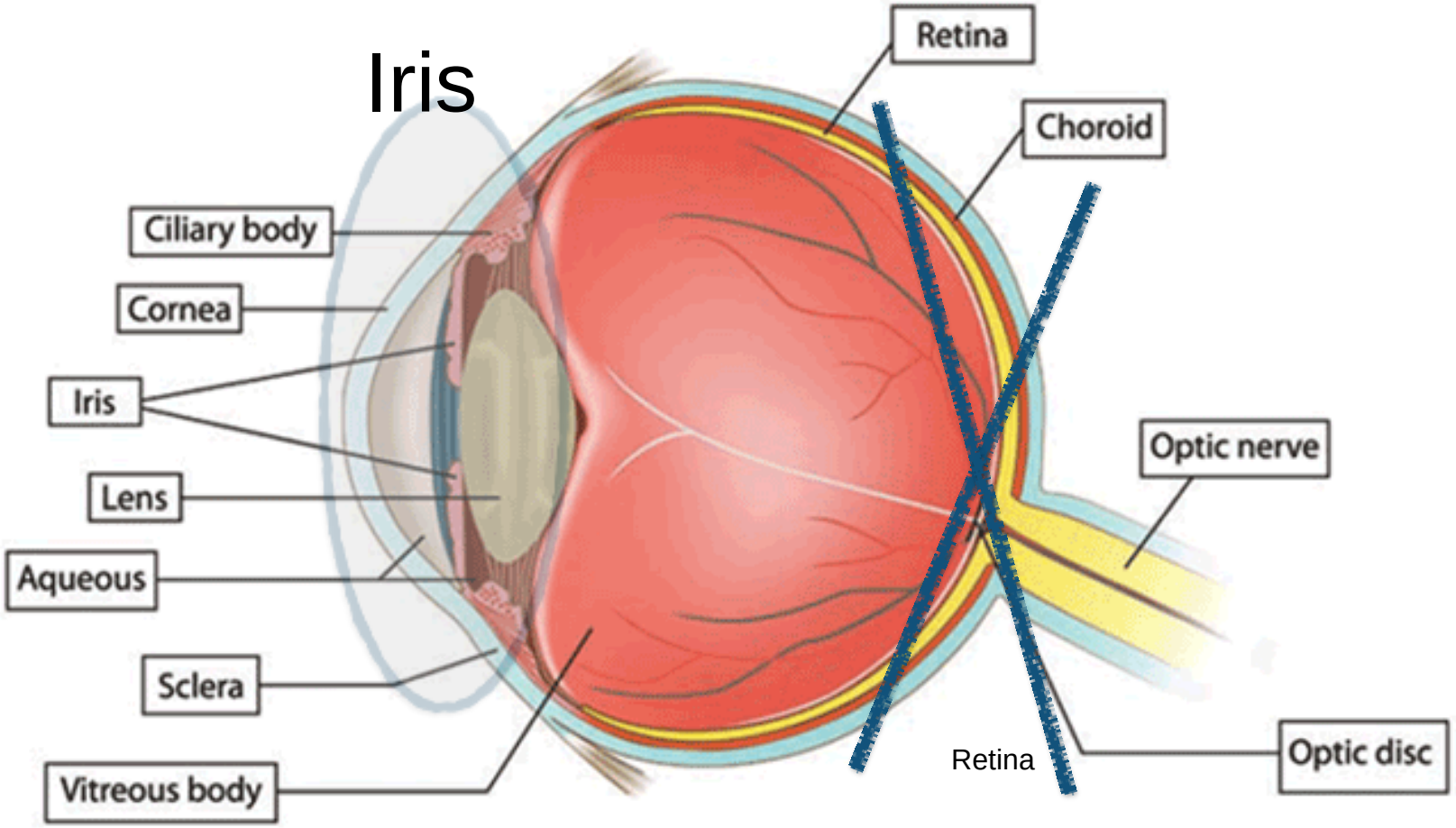
- 200 degrees of freedom
- Iris cameras available from several manufacturers, patterns scanned are interchangeable
- Can be done from a distance, but need to get a good picture of the irises
- Doesn’t require excessive lighting.
- Can image in the infrared, so easier to capture image
- 25+ hospital systems around the US

Limitations of iris scanning

- Psychology – patients think you are taking a picture of their face – concerns by undocumented immigrants
- Confusion with retinal scanning
- Pigment dispersion syndrome (rare, but it does occur)
- Hardware more costly than some other devices

Reviewing eye anatomy

Iris



Imaging iris, NOT retina !!

Fingerprint

»

- Has been used for decades in many industries/domains
- Many different sensing technologies, which continue to improve
- Advantages: a fingerprint captured on one technology device will be usable on other technologies
- Two components: print capture, software processing
- A technology that has been well accepted in some healthcare domains
  - Multi-layer (3D) technology – images not only finger ridges, but also subcutaneous tissue
  - 3-dimensional readers appear to be the most reliable. Although more expensive, they can distinguish reality from spoof, living from not, etc.

Fingerprint applications

»

- Regional blood centers (more than four) are now using fingerprint to identify their donors
- Extensive use in healthcare applications internationally
- Robust use outside of patient identification
  - The iPhone !!
  - PC Logon
  - Health club check in
  - Registration for the Haj
  - Many security/access control applications
  - Healthcare system single sign on
  - ATM machines in several countries

Limitations of fingerprint

- Psychology: Some of US population associates fingerprint with police work – so those patients who many not want to be identified to the police (e.g., undocumented immigrants) may decline to participate
  - For this reason (concern about patient misgivings) some health systems have chosen to use a different biometric
- Physiology: finger ridges not well developed in early childhood, skin character changes in elderly. Stone masons wear ridges off, so may have to use a different tool in those populations
- Device dependence – cheap devices can be spoofed
- Articles on limitations of fingerprint are typically talking about cheap, crude devices

Palm Vein Technology

Visible light

Near-infrared light

Extracted vein pattern

Palm vein

»

- Developed by Fujitsu, Japan, early 2000’s
- Introduced into US healthcare in 2007
- Veins in your palm visualized in the infrared
- Algorithm converts these into a unique identifier
- Has been used in many settings other than healthcare
- ATMs
- Home safe access

Palm vein implementations

- In active use at over 30 health systems
- Most: patient registration area, physician's offices
- Some: outpatient laboratory, draw stations
  - BayCare Health Systems, Tampa,
  - University of Wisconsin
  - Carolinas Healthcare,
  - Harris County Health
  - Michigan health information network
- Expanding to outside physician's practices that refer specimens
- Separate "template" used for each client network
  - so an identifier from one health system is not directly usable by others
  - increases security, but ….
  - for ability to consolidate across networks, have to add special programming

Case study: BayCare Health System (a palm vein site)

»

- Cost savings from reduction of duplicate medical records alone

- 30,300 deceased to 17,633 = 12,667 less duplicate records
- Cost/FTE (fully loaded) = $18.75 per hour
- Time needed to research and merge = 40 minutes per record
- Cost to correct = $12.50 per record
- Cost savings 1st year - just from avoided duplicate = $158,337

Palm vein - limitations

- »Psychology - some have raised the concern that the reader could be a fomite - but it is no more so than any hospital door knob.
  - Nevertheless, alcohol wipes are used by many hospitals
- »Positional
- »Susceptible to outside light (e.g., sunlight in Brazil - ATM's)
- »Templates are specific to each contract/organization, unless comparability programming is added
- »Palm veins develop until about age 5
  - Necessary to re-image each year.

Avoiding door knobs in hospitals

»

Signature biometric

- A behavioral biometric - Device senses the tempo and geometry of a signature - not the final product
- Quite specific, have been extensively used in education.
- All of the anatomic biometrics: Iris, fingerprint, palm vein, face recognition, etc. - are immutable
  - If the channel from the biometric reader to the database is penetrable, then in theory the ID could be hacked (I'm not aware of such a case)
- Advocates of signature argue that there are advantages to a mutable biometric
  - Signature can, by force of will, be changed - so if your anatomic biometric were compromised, you could use a behavioral biometric, the could be changed at will.
- .

A fallback strategy

- Whichever biometric you choose as your primary identifier, there will be a small percentage of patients for which it will not work:
  - Fingerprints in stonemasons
  - Signature biometric for a comatose patient
  - Palm vein for a hand amputation
- Given this, a defined fallback strategy must be defined - preferably, a second biometric (e.g., use fingerprint for a patient with pigmentary dispersion of the iris)
- Some health systems will choose to measure two biometrics for each patient. This provides even better precision, and a built-in fallback strategy (e.g., a method for the comatose patient0

Where do we station biometric readers?

- Patient registration
- Inpatient admitting
- Outpatient registration
  - Self check-in kiosks
- Lab draw stations
- Physician's offices (especially if collecting specimens)
- In each of these, it may be necessary to generate a wristband (barcode or RFID) closely linked to biometric identification

- Another philosophy - for patients without other reasons for wristbands (e.g., outpatient labs), place biometric reader at every draw chair.

Need more than just a biometric reader

- One or more biometric technologies
- A server to manage both primary (biometric) identifiers, as well as secondary identifiers
  - Text identifiers
  - ID cards
  - Other tokens
- Such “back end” servers can increase security, facilitate linkage with other organizations, etc.
- Security: important to protect the connection between biometric readers and the identification database
  - Theoretical risk of inserting spoofed electronic signature without an actual biometric read

Biometrics are not a panacea

»

- Require special equipment - cost, logistics
- Psychological/sociological -
  - Fomite
  - connotations of fingerprinting - law enforcement
  - Counterexamples - iPhone, health clubs
- Some biometrics may not work well in certain populations - e.g., fingerprints in newborns, and in some of Asian descent, palm vein if less than 5 years old
- Skeptical patients
- Disuse - a management issue

Skeptical patients?

- In most health systems, less than 1%
- Provide a brochure explaining how the scan will improve care of the patient
- Registrars apply subtle persuasion - “why aren’t you registered in the biometric safety system?”
- Some have proposed (!) that those who refuse be asked to sign a waiver, confirming that they understand they are placing themselves at higher risk of adverse consequences (death and dismemberment)

Strengths of biometrics

»

- Ability to reliably discriminate among millions of people
- Don’t require patient to remember several surrogate identifiers
- Safeguards against intentional misidentification
- Will not change, cannot be impersonated, will remain with the patient over years
- Avoid costs and dangers of merging

Questions

Raymond D. Aller, M.D.
raller@usc.edu
760-801-3760