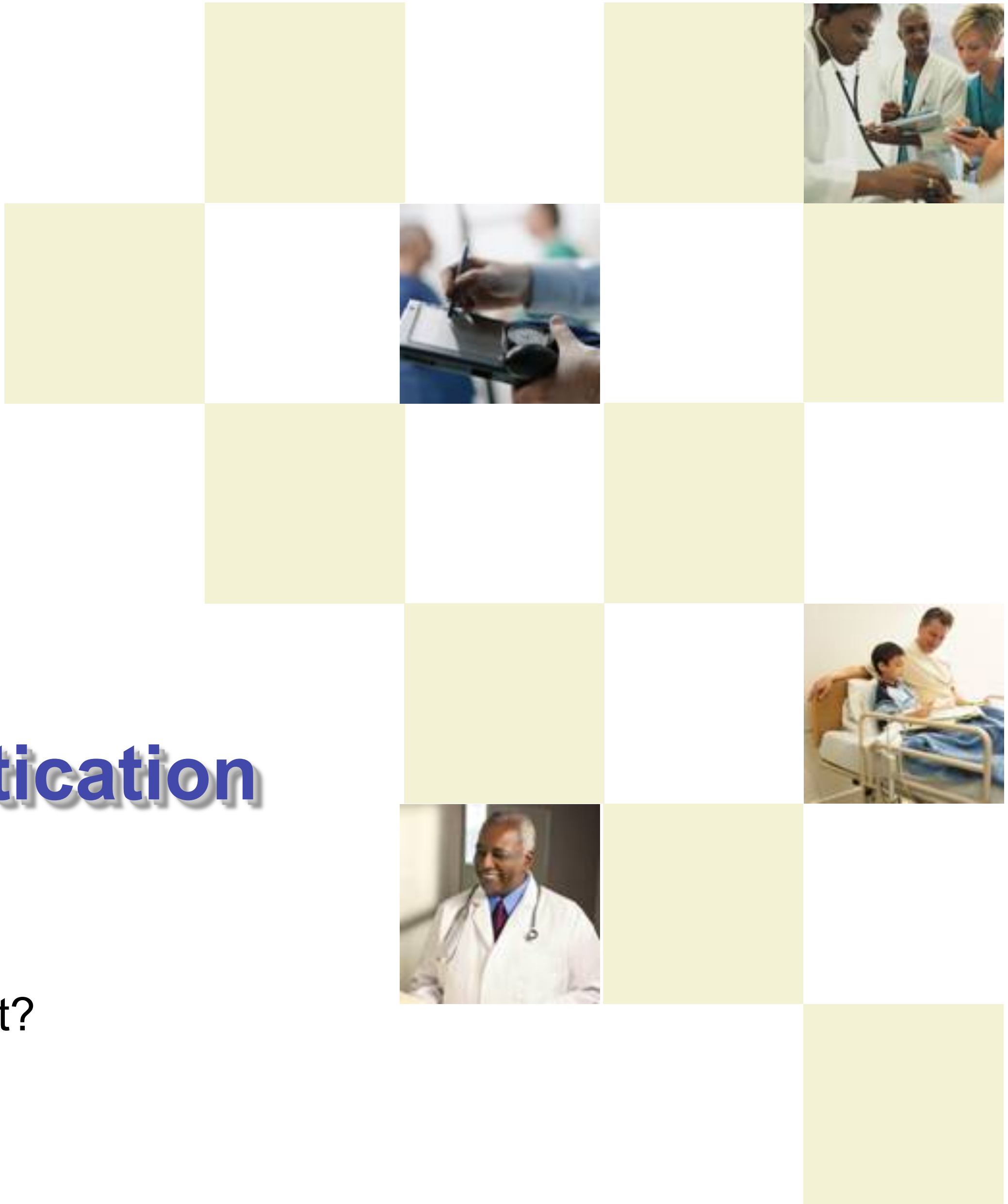
SAFE-BioPharma®

SAFE-BioPharma Association



Healthcare Authentication

What's it all about?

Topics

- **ONC HIT Standards Committee**
- **ASTM Standards**

SAFE-BioPharma®

SAFE-BioPharma Association

ONC HIT Standards Committee

- **Oct 21st meeting Security & Privacy Consumer Communications Recommendations**
  - Use at least one factor (e.g., password) to authenticate the identity of consumer or personal representative
  - Exchange messages securely
    - Authenticate consumer
  - Authentication: Separate criteria for person vs. entity
    - Person authentication - at least single factor (e.g. user name & password)
    - Entity authentication – X.509 certificates
  - Two-factor authentication is out of scope (???)
  - Access control. Assign a unique name and/or number for identifying and tracking user identity and establish controls that permit only authorized users to access electronic health information.
    - IMPLEMENTATION SPEC: ASTM, E1986-09 (Information Access Privileges To Health Information)

ASTM Standards

- IMPLEMENTATION SPEC: ASTM, E1986-09 (Information Access Privileges To Health Information)
  - References ASTM, E1869 – 04 (Reapproved 2010) Standard Guide for Confidentiality, Privacy, Access, and Data Security Principles for Health Information Including Electronic Health Records
    - Further references: Designation: E1762 – 95 (Reapproved 2009) Standard Guide for Electronic Authentication of Health Care Information

- Among other things, Defines minimum requirements for user identification, access control, and other security requirements for electronic signatures
- User authentication is used to identify an entity (person or machine) and verify the identity of the entity. Data origin authentication binds that entity and verification to a piece of information. The focus of this standard is the application of user and data authentication to information generated as part of the health care process. The mechanism providing this capability is the electronic signature.

SAFE-BioPharma®
SAFE-BioPharma Association

Standard Guide for Electronic Authentication of Health Care Information

- The guide addresses the following requirements, which any system claiming to conform to this guide shall support:
  - Non-repudiation,
  - Integrity,
  - Secure user authentication,
  - Multiple signatures,
  - Signature attributes,
  - Countersignatures,
  - Transportability,
  - Interoperability,
  - Independent verifiability, and
  - Continuity of signature capability
- There are no recognized security techniques that provide the security service of non-repudiation in an open network environment, in the absence of trusted third parties, other than digital signature-based techniques

SAFE-BioPharma®

SAFE-BioPharma Association

Standard Guide for Electronic Authentication of Health Care Information

- User Authentication
- User Authentication with Passwords – severe limitations, security that passwords provide is dependent on the manner in which they are used, but generally the common practice of simple user entry of passwords is inadequate to meet the intent of an electronic signature
- Other means – secret key, public key, biometric
- Token-based User Authentication—User authentication is commonly based on one or more of the following attributes:
  - something you know,
  - something you possess, and
  - something you are

SAFE-BioPharma®

SAFE-BioPharma Association

So what should it look like?

- Cited ASTM Standards clearly point to strong two-factor authentication for access to healthcare information on the part of medical professionals

SAFE-BioPharma®

SAFE-BioPharma Association

Authentication and credentials

- **PKI is covered by the FBCA CP and CPS**
  - Multiple certificate types
  - Hardware, software and roaming
    - Roaming currently classed as software by the FBCA
    - Moving to cloud-based solutions – SAFE-BioPharma/Verizon offering cloud-based HSM protected certificates
- **Non-PKI**
  - NIST SP 800-63
  - Issue – currently approved version dates to 2006 and is technically out of date and does not recognize non-PKI multi-factor tokens
  - Much of industry working with the Dec 2008 (now Jun 2011 draft)
    - Includes much broader definitions of acceptable tokens at various LOAs

Token types

- **Who is doing what and how?**
- **PKI**
  - Smartcards, USB hardware tokens, software tokens on machines/ mobile devices, cloud HSMs
- **Non-PKI**
  - LOA 1&2 – memorized secrets, pre-registered knowledge tokens
  - LOA 2 - look up secret, out of band, SF one-time password device, SF crypto device
  - LOA 3 – multiple tokens (NIST SP 800-63 (June 2011 draft), Table 7)