MedicAlert®

Workgroup on the National Health Information Infrastructure (NHII)

Subcommittee on Privacy

February 24, 2005

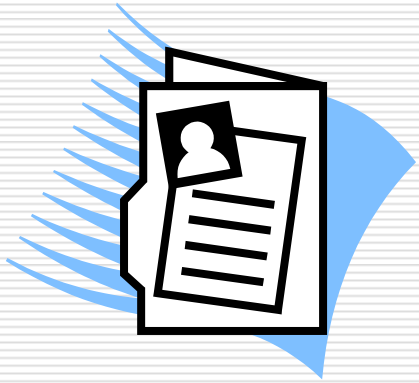
NCVHS

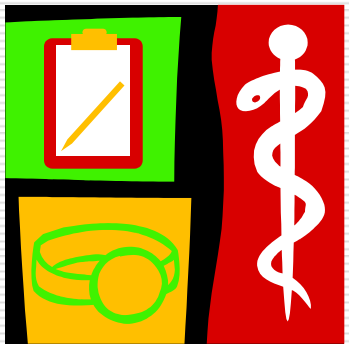
Our Philosophy

The business of MedicAlert® is to protect and save lives. We enhance patient safety and improve quality of care, by providing secure data collection and storage with accurate and easy transfer of medical information to health and safety professionals 24 hours a day, anywhere in the world.

MedicAlert® Services

- Personal Electronic Health Records
  - MedicAlert® has developed an EHR for managing medical information for our members
  - The EHR is designed to be compatible with healthcare industry standards and the data will come from many different sources
  - The CapMed PHR product will allow members to maintain their own records with bi-directional updates to and from the MedicAlert® EHR
  - Records are accessible from the MedicAlert Web site, from the MedicAlert® USB Personal Health Key software, or by calling the MedicAlert® Contact Center





MedicAlert® Services

- Document Repository Services
- Professional Education & Training
- Member Education
- FDA Approved Medical Device/Implants Registry
- Family Notification Services

Privacy and Confidentiality Today

- All personal and medical data is provided directly by our Members
- MedicAlert® obtains prior written approval for all storage and transfers – electronic or otherwise – of Members' personal data
- The MedicAlert® Emergency Response Team follows a proprietary 10-step Responder Identification Protocol for all incoming Emergency Calls
- The MedicAlert® Web site uses the following process and technology components to safeguard member medical information privacy:
  - Member Number / Password combination for access
  - Additional member-selected elements for identification and authorization
  - Secure, encrypted transfer of information

MedicAlert® EHR Interoperability

- Next generation Enterprise Architecture will include the HL7 RIM and functionality that maps to the EHR Functional Outline, and emerging OMG-HL7 Service specifications for EHR interoperability
- Expanded scope of information sources for our membership will drive interoperability with provider EHRs, payers, labs, etc.
- Expanded scope of drug utilization reviews drive interoperability requirements with chain drug stores, pharmacies and PBMs
- Management of patient-directed authorization for release of information will also drive requirements for interoperability

Privacy and Security Tomorrow

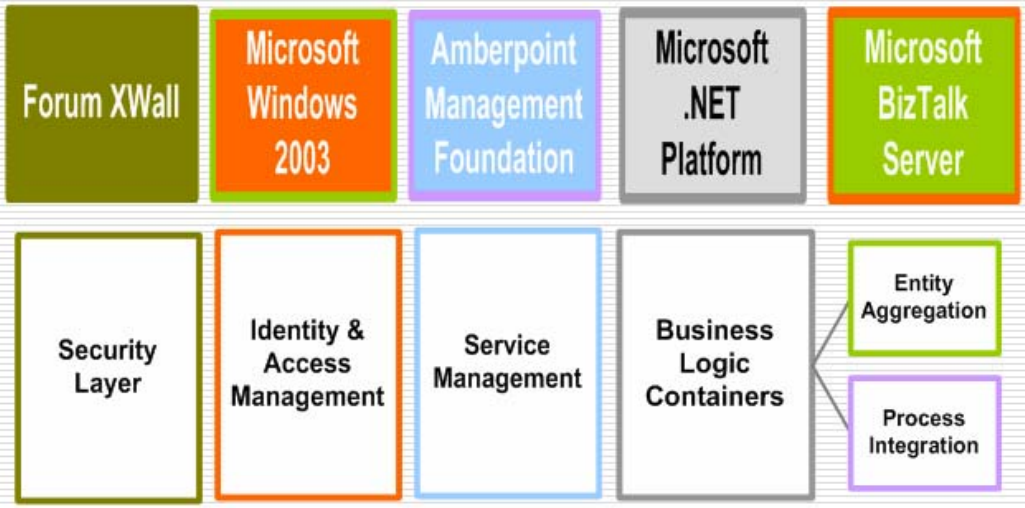
- The following enhanced security measures are in various stages of deployment:
  - Multi-tiered data access authorization
  - Internal network domains include software and hardware firewalls
  - Internal hacking and intrusion detection
  - Every data access generates an audit trail
  - Application of regular and extensive “password guesser” algorithms
  - No unencrypted XML data
  - All externally accessed hardware in a DMZ
  - No unencrypted login across machines
  - Data source notations (e.g. patient entered or medical professional entered)

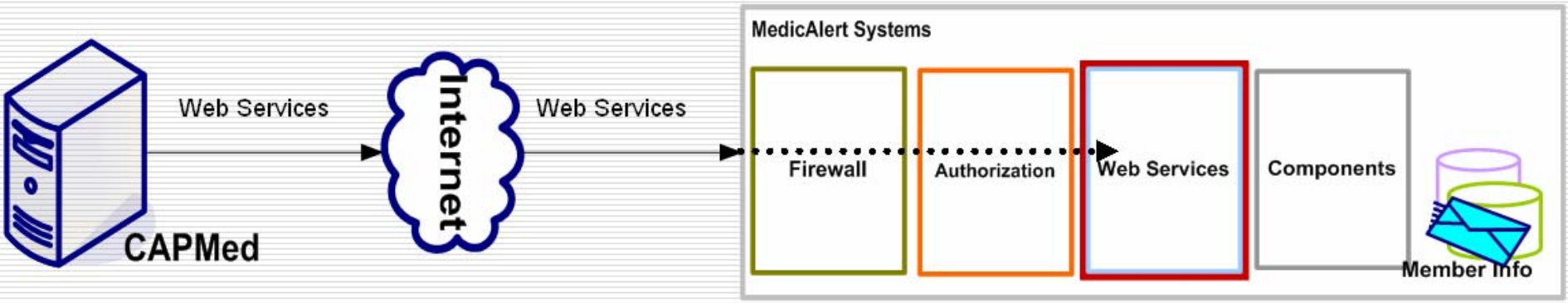
MedicAlert® Security Architecture

Technology Products

http://www.medicalert.UpdateMyRecord.asmx

Technology Concerns





Privacy – Upcoming Issues

- Authorization management, since much of our potential business with payers, PBM's, employers, etc. falls outside the direct medical care umbrella.
- Authorization of emergency responders for release of information
- Member support and education on the implications of withholding or releasing information under different circumstances

Authorization Management

Members must be in control of data sharing between MedicAlert® and our current and future partners:

- Provider Electronic Health Records
  - Expanded scope of data collection
  - Availability of medical data to providers
  - Downloadable to the PHR
- Payers
  - Expanded scope of data collection
  - Out of network notifications
- Employers
  - Health and wellness reporting
  - Occupational Health
- Pharmacy Benefits Managers and Retail Pharmacies
  - Expanded scope of drug utilization reviews
  - Drug interaction checking
  - Adverse Event Reporting
- Laboratories
  - Expanded scope of data collection
  - Downloadable to the PHR

Role-Based Access Privileging

- Services Specification Project
  - HL7 and OMG HDTF collaboration
  - Technical requirements for interoperability
- Functional Requirements
  - Standard list of common roles
  - Common situations/contexts
  - Guidelines for policies
- Authorizing emergency responders
  - ? Use of provider/facility ID's

Consumer Education/Counseling

- Implications of Withholding Release of Info
  - What may not be relevant in what situations
- Implications of Releasing Info
  - What may be relevant in what situations
- Requires healthcare professionals to counsel patients regarding their particular situations and objectives
  - Who? When? Where?

MedicAlert® Community

Consumers

Government

Hospitals

MedicAlert®

Physicians

Pharmacies

Public Safety

Clinical Trials