



# Access Control Techniques

Joel Russell

June 19, 2003



# Objectives

- Describe existing VistA Access Control infrastructure
- Explain Access Control framework planned for CPRS-R



“Back in *the Day*...When C. Everett Koop was ‘the bomb’...”

- Dumb Terminal Applications
- Single-tiered Architecture
- Homogeneous (Single Language) Programming Platform
- Access Control was determined by:
  - FileMan Access Codes
  - Options
  - Security Keys
  - Protocols
  - Attributes of People (e.g., AUTHORIZED TO WRITE MED ORDERS, etc.)



# Option Types

- *Action*
- *Edit*
- *Inquire*
- ***Menu***
- *Print*
- *Run routine*
- Protocol
- Protocol menu
- *Extended action*
- Server
- Limited
- ScreenMan
- Window
- Window Suite
- ***Broker (Client/Server)***



# Options and Access Control

- Menus (and Extended Actions)
  - Grouped hierarchically
  - Nested Indefinitely (cycles prohibited)
  - Invoke or allow selection of other Option types (e.g., action, run routine, etc.)
  - Provide a framework of navigation
  - Define the “path” to all functionality that the user may access



# Security Keys

- Confer permission to execute “locked” options
- May be allocated/removed from individual users
- Allocation could be distributed by identifying “delegates” outside IRM
- Security Keys were sometimes used to identify members of important groups (e.g., PROVIDERS)



## Options, Keys, “Roles”, and “Permissions”

- A user’s “role” within the local organization could be loosely inferred from their Primary Menu (e.g., AKF CHARGE NURSE MENU, etc.)
- Their “permissions” could be deduced from the intersection of their menu path with the keys which they held
- No API exists to compute such inferences



# Options & Keys for Access Control

## *Pros*

- Flexible & Extensible
- Familiar to system administrators with various skill sets
- Supported Operation-Based Access Control in 1-Tier apps well

## *Cons*

- No direct API for Access decisions
- Doesn't port fully to 2-Tier or n-Tier apps
- Binds UI to Business Logic to Data Layer
- Local extensions w/o mapping to any enterprise standard



# Enter Client/Server

- Option trees no longer meaningful for most AC functions
- Transactions (RPCs) needed to calculate/return access decisions
- Broker type Options Introduced
  - Allowed registration of accessible operations (RPCs) within specific Options



# Authorization/Subscription Utility

RBAC for CPRS v1



# Functional Overview

- Document (Object) & User Class (Role) Hierarchies
- ASU's Declarative Model
  - How Rules are made
- ASU's Inference Model
  - How Rules are evaluated



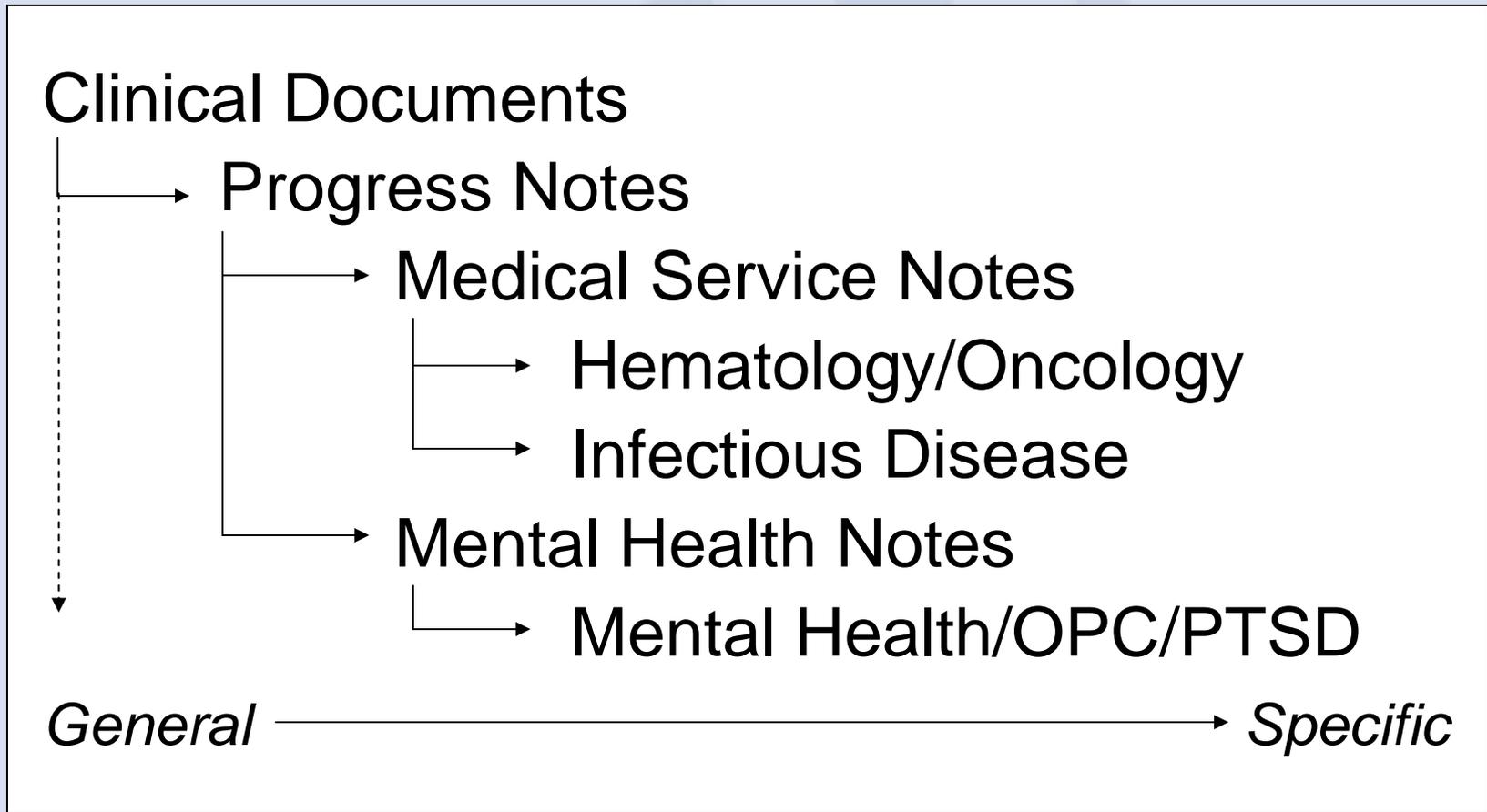
# Modeling Reality With Object-Oriented Design

**“It’s important to realize that you’re interested less in *individual objects* than in *abstract types* of objects. When you create a type, you need to imagine *not* the *specific case*, but the *general case*. If you’re modeling a system that needs to describe employees, create a type that represents the general class of employees and go from there, creating instances and deriving subtypes.”**

**- Gary Entsminger *The Tao of Objects*  
2<sup>nd</sup> ed. 1995**

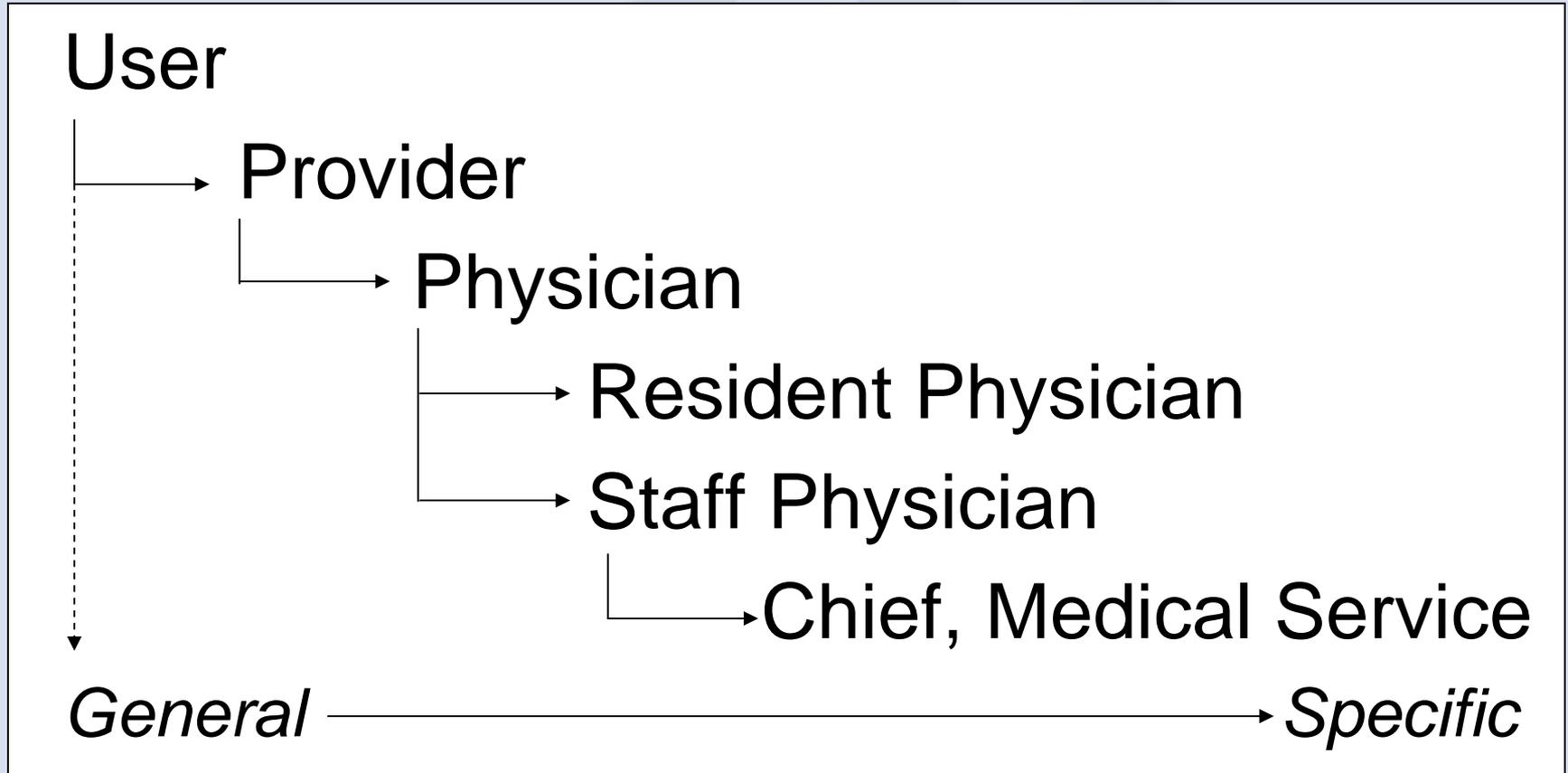


# Document Definition Hierarchy





# User Class (Role) Hierarchy





## ASU's Declarative Model (Managing Permissions)

“Can this user perform this action (operation) on this document in its current state?”

- Table of rules defined by five properties:
  - Document Definition (object)
  - Status
  - Action (operation)
  - User Class (role)
  - User's Role (relationship to object)



# ***“Rules?! We Don’ Need No Stinking Rules!”***

## *General*

An UNSIGNED (CLASS) CLINICAL DOCUMENT may be EDITED by An AUTHOR/DICTATOR

An UNCOSIGNED (CLASS) DISCHARGE SUMMARY may be COSIGNED by A STAFF PHYSICIAN who is also An EXPECTED COSIGNER

An UNTRANSCRIBED (DOCUMENT CLASS) NURSE’S NOTE may be ENTERED by A NURSE

An UNCOSIGNED (TITLE) PULMONARY CONSULT may be EDITED by A STAFF PULMONOLOGIST

## *Specific*



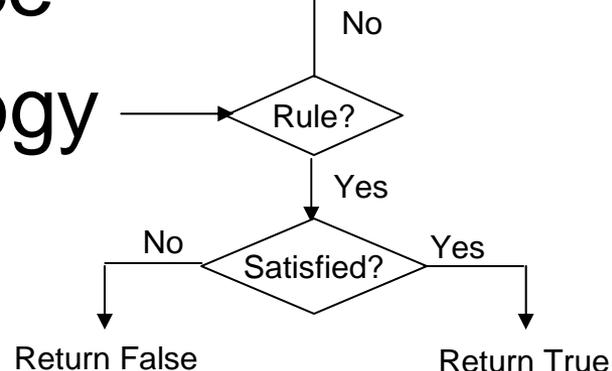
# ASU's Inference Model: Single Inheritance & "Trickle-up"

Clinical Documents

└─> Progress Notes

└─> Medical Service

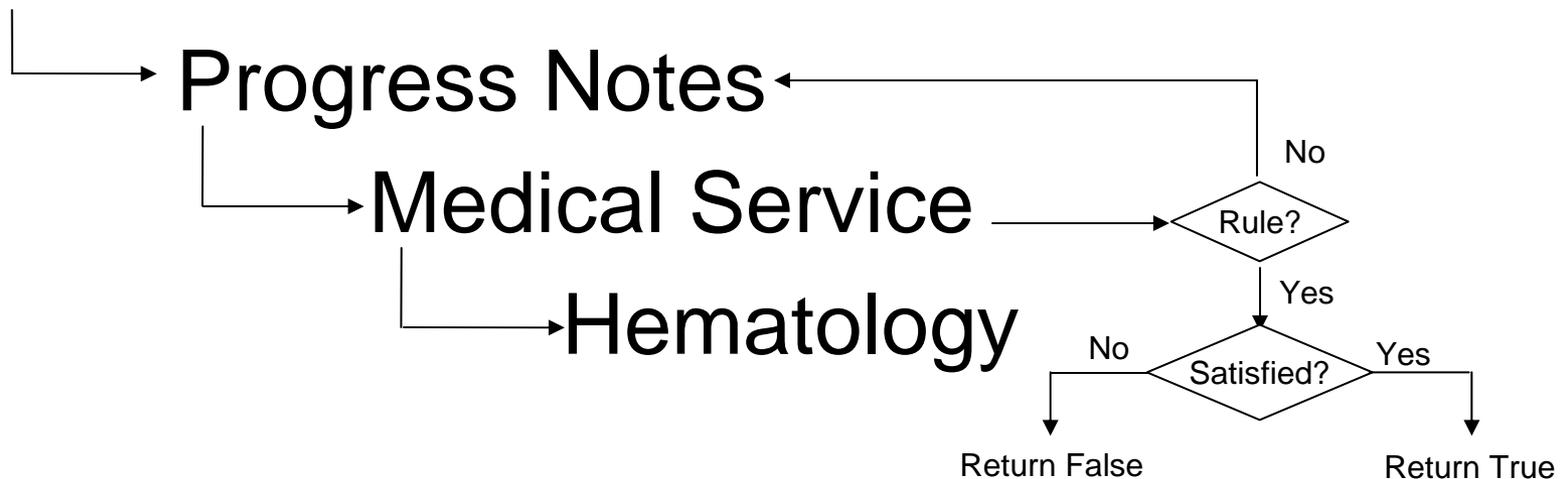
└─> Hematology





# Okay, I've Upped My Attitude...

## Clinical Documents





# ASU for Access Control

## *Pros*

- Flexible & Extensible
- Well-suited to Client/Server
- Supports Core RBAC
- Supports Hierarchical RBAC
- Supports declaration of business rules
- Models Health Care workflow well

## *Cons*

- *Currently* - Only applies to Documents
- *May* be difficult to port to Oracle
- Needs mechanism for specifying negation / prohibition
- Needs log-in context to support multiple membership better
- Local extensions w/o *guaranteed* mapping to any enterprise standard



# CPRS Re-Engineering

Access Control for HealthVet  
Desktop & Care Management



# HealthVet Desktop Definition

- HealthVet Desktop is the new environment for hosting VistA graphical interfaces
- Care Management provides first four perspectives
- Hosts CPRS-R
- Future VistA applications

The screenshot displays the HealthVet Desktop interface. The title bar reads "HealthVet Desktop in use by: GEARY, JOREL (isl-reengkm:8000)". The interface includes a menu bar (File, Edit, Tools, Action, Help) and a toolbar. A table at the top lists patients with columns for Patient, Rst, Task, Evt, and Sign. Below the table, a patient record for APPLESEED, JOHNNY is shown, including contact information, address, and clinical details.

Patient	Rst	Task	Evt	Sign	Patient	Rst	Task	Evt	Sign
AAA,PATIENT					BABBIT,VERONA				
ANDERSON,H C					BABBITT,GEOR...				
APPLESEED,JO...					BABBITT,KATHE...				

APPLESEED,JOHNNY 466-68-0999 30 Apr 1944 (59)

APPLESEED,JOHNNY 466-68-0999 APR 30,1944  
-----  
COORDINATING MASTER OF RECORD: NOT LISTED

Address: 230 NORTH 7TH EAST Temporary: NO TEMPORARY ADDRESS  
BAY PINES, FL 02134

County: DADE (25) From/To: 1738 -  
Phone: UNSPECIFIED Phone: NOT APPLICABLE  
Office: UNSPECIFIED Rx Mail Delivery: REGULAR MAIL  
Relig: PROTESTANT, NO DENOMINATION Sex: MALE  
Race: WHITE, NOT OF HISPANIC ORIGIN  
POB: VIETNAM ERA Claim #: 466680999

Primary Eligibility: NSC, VA PENSION (NOT VERIFIED)  
Other Eligibilities: HUMANITARIAN EMERGENCY

Status : ACTIVE INPATIENT-on WARD (Seriously ill)

Admitted : MAY 11,1999@08:23:36 Transferred : MAY 24,1999@14:27:18  
Ward : 2B MED Room-Bed :  
Provider : BAYLIS,RANDALL Specialty : NEUROLOGY OBSERVATION  
Attending : BAYLIS,RANDALL



# A User's View of the Desktop

Perspective Selector

Patient	Rslt	Task	Evnt	Sign	Patient	Rslt	Task	Evnt	Sign	Patient	Rslt	Task	Evnt	Sign
AAA,PATIENT					BABBIT,VERONA					BENOIT,JEAN				
ANDERSON,H C					BABBITT,GEOR...					JONES,ARNOLD				
APPLESEED,JO...					BABBITT,KATHE...									

APPLESEED,JOHNNY 466-68-0999 30 Apr 1944 (59)

APPLESEED,JOHNNY 466-68-0999 APR 30,1944

-----  
COORDINATING MASTER OF RECORD: NOT LISTED

Address: 230 NORTH 7TH EAST Temporary: NO TEMPORARY ADDRESS  
BAY PINES, FL 02134

County: DADE (25) From/To: 1738 -  
Phone: UNSPECIFIED Phone: NOT APPLICABLE  
Office: UNSPECIFIED Rx Mail Delivery: REGULAR MAIL  
Relig: PROTESTANT, NO DENOMINATION Sex: MALE  
Race: WHITE, NOT OF HISPANIC ORIGIN  
POS: VIETNAM ERA Claim #: 466680999

Primary Eligibility: NSC, VA PENSION (NOT VERIFIED)  
Other Eligibilities: HUMANITARIAN EMERGENCY

Status : ACTIVE INPATIENT-on WARD (Seriously ill)

Admitted :  
Ward :  
Provider :  
Attending :

Perspective

Visual Component

The desktop hosts visual components, organized into perspectives



# Definitions

- **Perspective:** A view into the data configured to support workflow
- **Perspective Selector:** Choice of perspectives available to the current user
- **Visual Component:** Reusable pieces that operate inside a perspective



# Desktop Characteristics

- Provides the client framework for a multi-tiered environment
- Allows flexible visual layout
  - Select and position components
  - Construct new perspectives (views)
- Provides a pluggable environment
  - Open model for contributing components
  - Dynamically assembled at startup
  - Inter-component communication supported



# Proposed Encounter Perspective

Perspective Selector

HealtheVet Desktop: Encounter Entry

File Edit View Action Tools Help

DAWSON, JAMES K. 326-44-6616 01/9/66 (36)

Problems Note Title Vitals

Note Work Area

Recent Labs

Reminders

Templates

Desktop allows custom configuraton of components into a single "perspective". For example, a custom perspective to document an encounter.

Encounter Perspective

Visual Component

Perspectives provide a user's view into the data based on their role or immediate tasks



# Advantages

- Customization for specific user roles and activities.
- Hosts locally developed and COTS plug-ins.
- Provides an environment that allows for dividing CPRS into reusable components
- Distributed development of components



# Configuring Desktop Options

- Today
  - Perspectives are mapped to options
  - Facilitates assignment and access
  - RPC access is managed by options
  - Document Access Control mediated by ASU
- Future
  - Enterprise security architecture (why we're here)
  - Well-positioned Service Oriented Architecture (e.g., JAAS, RBAC, LDAP)

