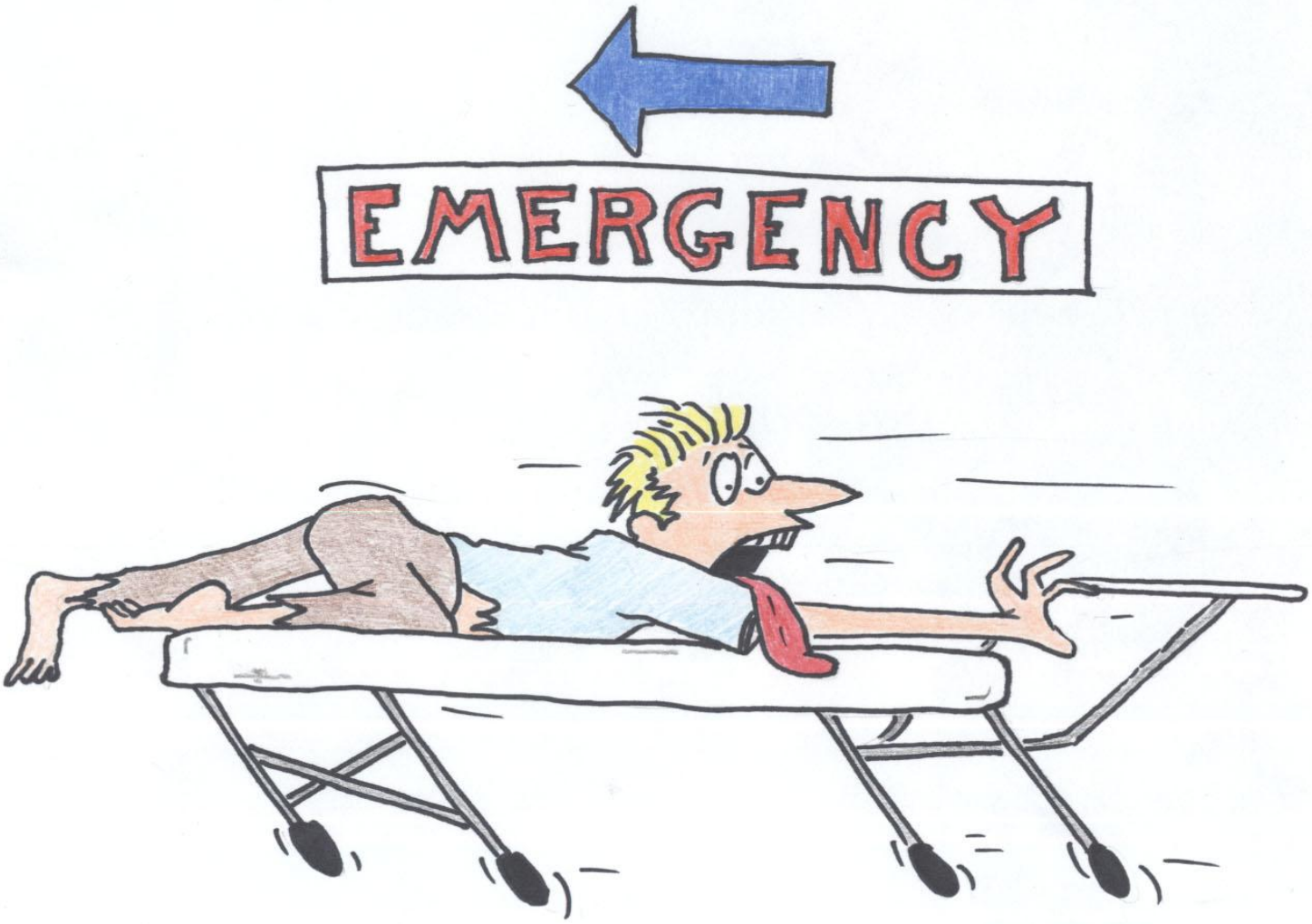
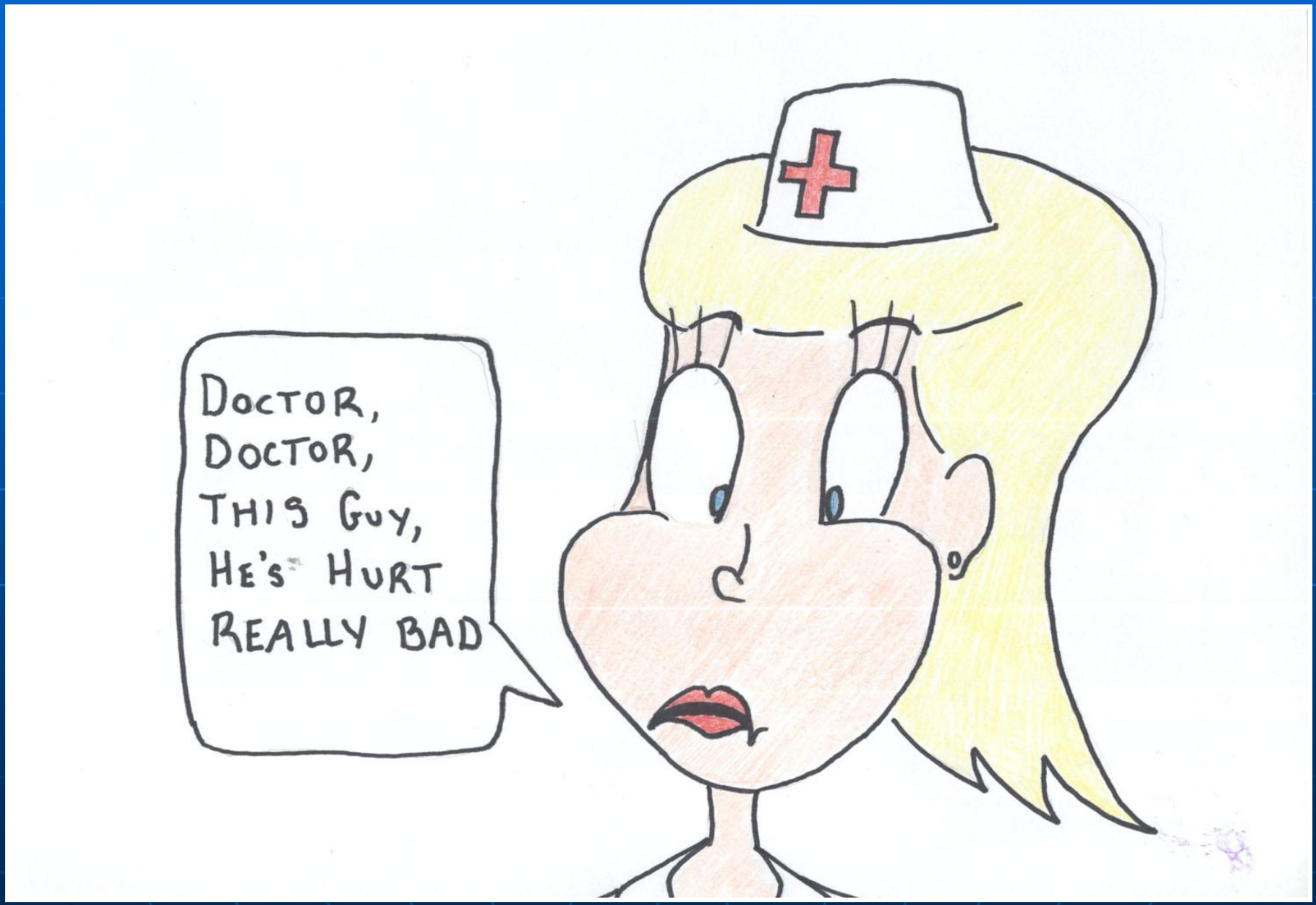

EMERGENCY

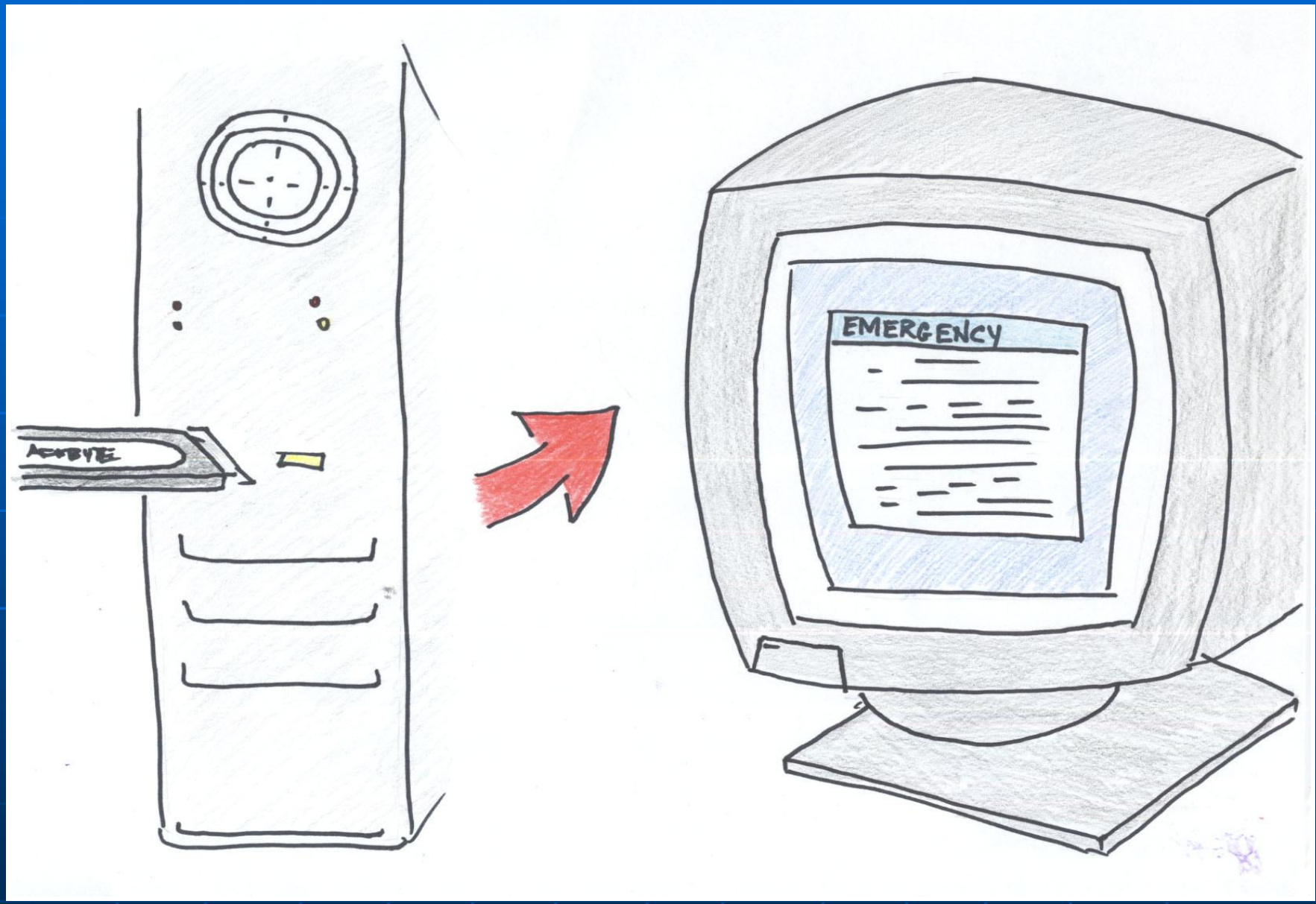

DOCTOR,
DOCTOR,
THIS GUY,
HE'S HURT
REALLY BAD


WHAT DO WE KNOW ABOUT HIM?


THAT'S THE PROBLEM, WE DON'T KNOW A THING. NO NAME, NO PREVIOUS HEALTH RECORDS, HECK, NO ENGLISH


WHAT ARE WE GONNA DO!?!?


SAFEBYTE
WAIT!
HE'S GOT
THE
SAFEBYTE

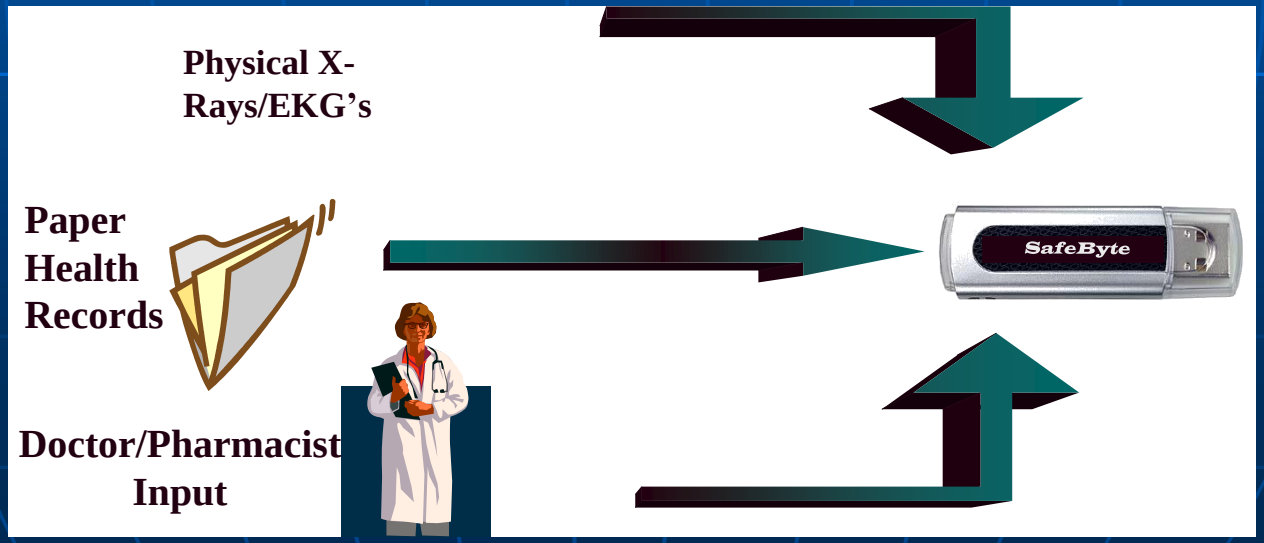

EMERGENCY


WITH ALL THIS INFO, WE'RE HOURS AHEAD OF SCHEDULE. LET'S GET STARTED!
OR 217


[MUMBLING]
THANKS
SAFEBYTE...

IPRO 304
SafeByte Health System

Portable and Secure Data Storage System



Names…. blah

What are we doing?

The goal of this project is to design software to support the secure use of portable memory as a medium for transferring secure data.

Objectives

Our Product will be:

- Portable
- Secure/Accurate
- Method of Authentication for software and data
- Cost-effective
- Easy to use
- Capable of having multiple users
- Compatible

Electronic Health Records

Benefits of EHR

- Immediate and Universal access
- Easier and quicker navigation
- No lost charts
- Standardization among health care providers
- Reduction of paperwork and documentation error
- Ability to transmit information to other providers

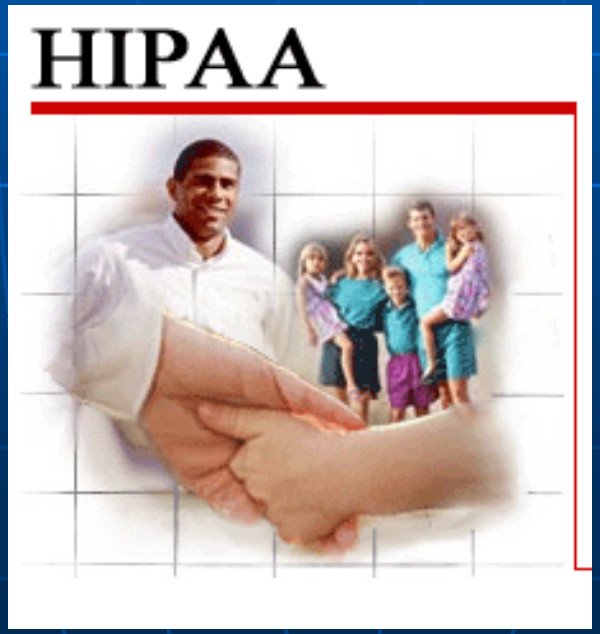
Why the delay?

- Privacy of patients record
- Lack of uniform Standards
- Time constraints
- For patients or insurers?
- Funding

HIPAA

Health Insurance Portability and Accountability Act

- Where Did HIPAA come from?
- Who sees the Medical Records?
- Guidelines to Being HIPAA Compliant.



How it relates to our Project?

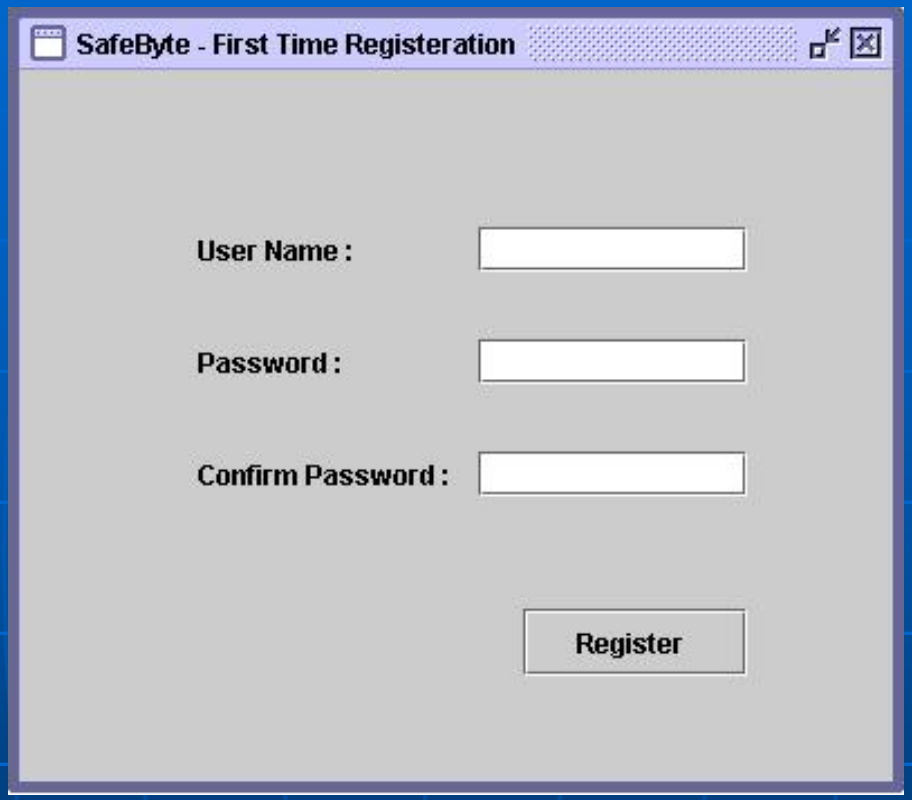
- Privacy of electronic records
  - Levels of Security~ Accessing and Editing
    - Doctors, Patients, Pharmacists, Insurance…etc.
  - Emergency Information
  - Access Logs~ Time stamps and Signatures
- HIPAA Compliancy

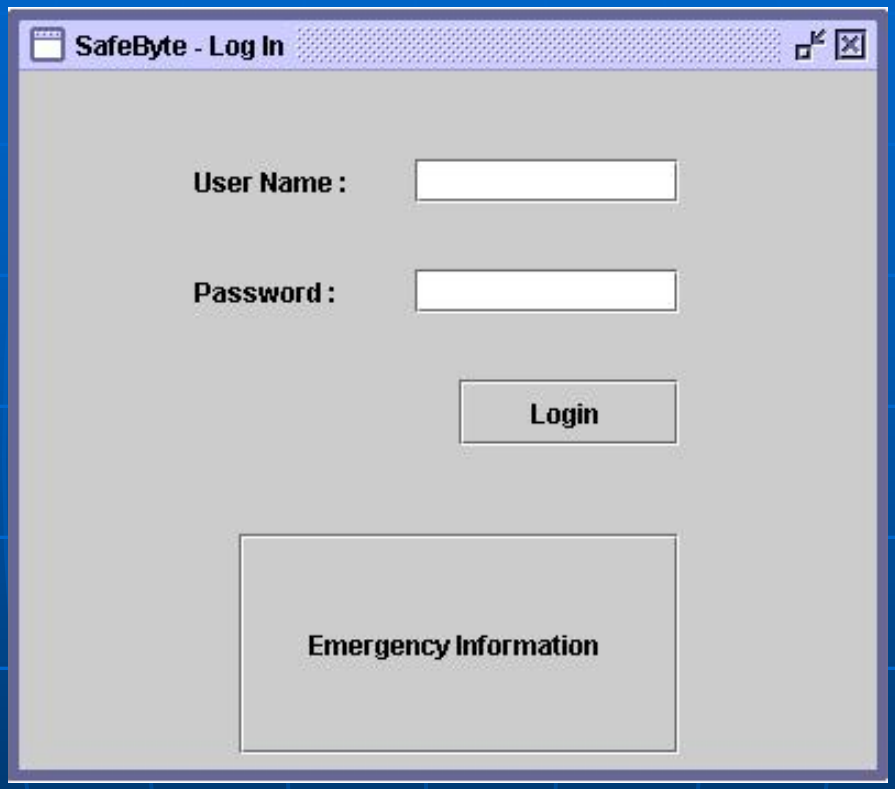
About the Program

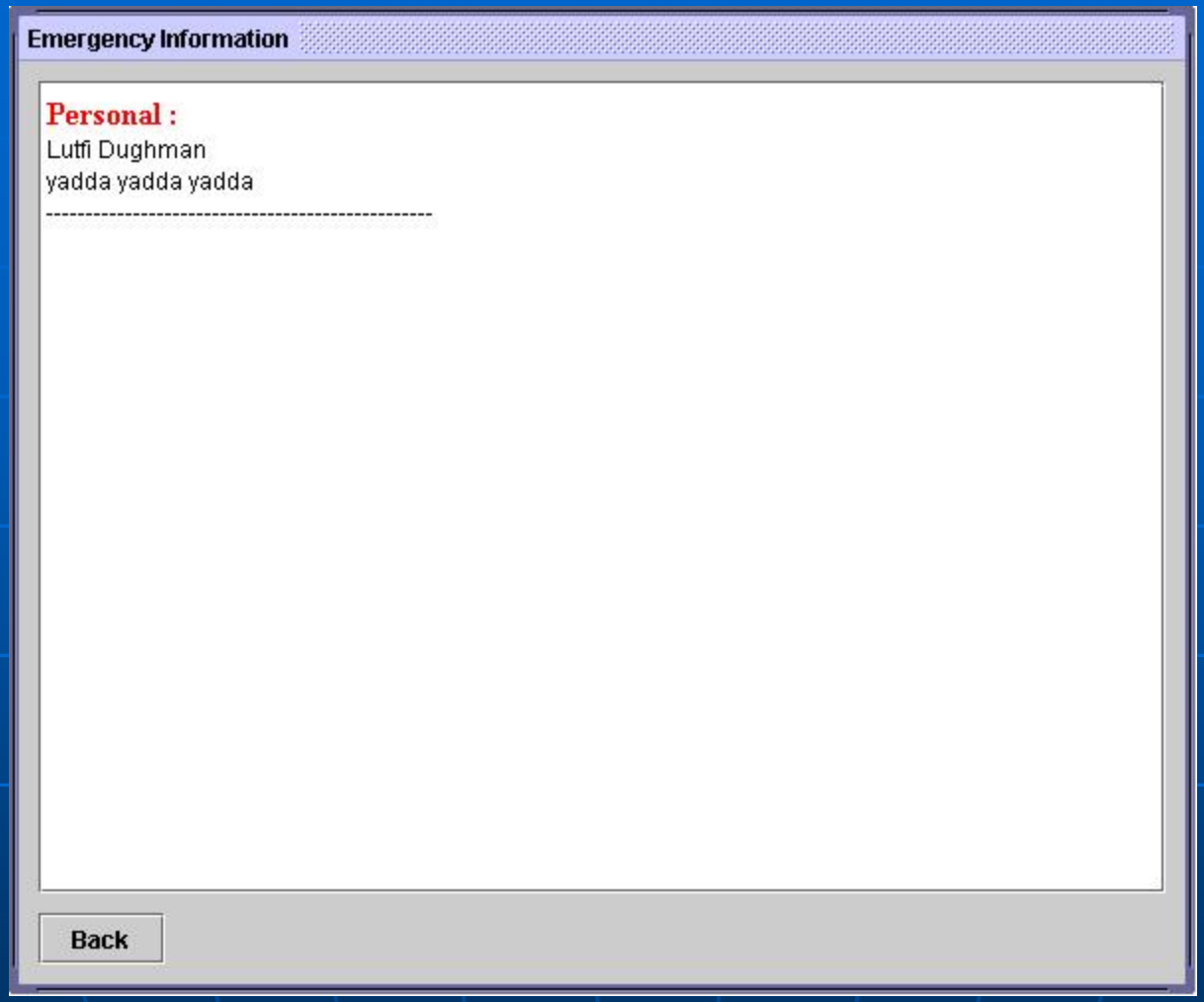
- Eliminates paper records
- Various types of Medical Information
- Multiple Users
- User Access Levels

User Matrix

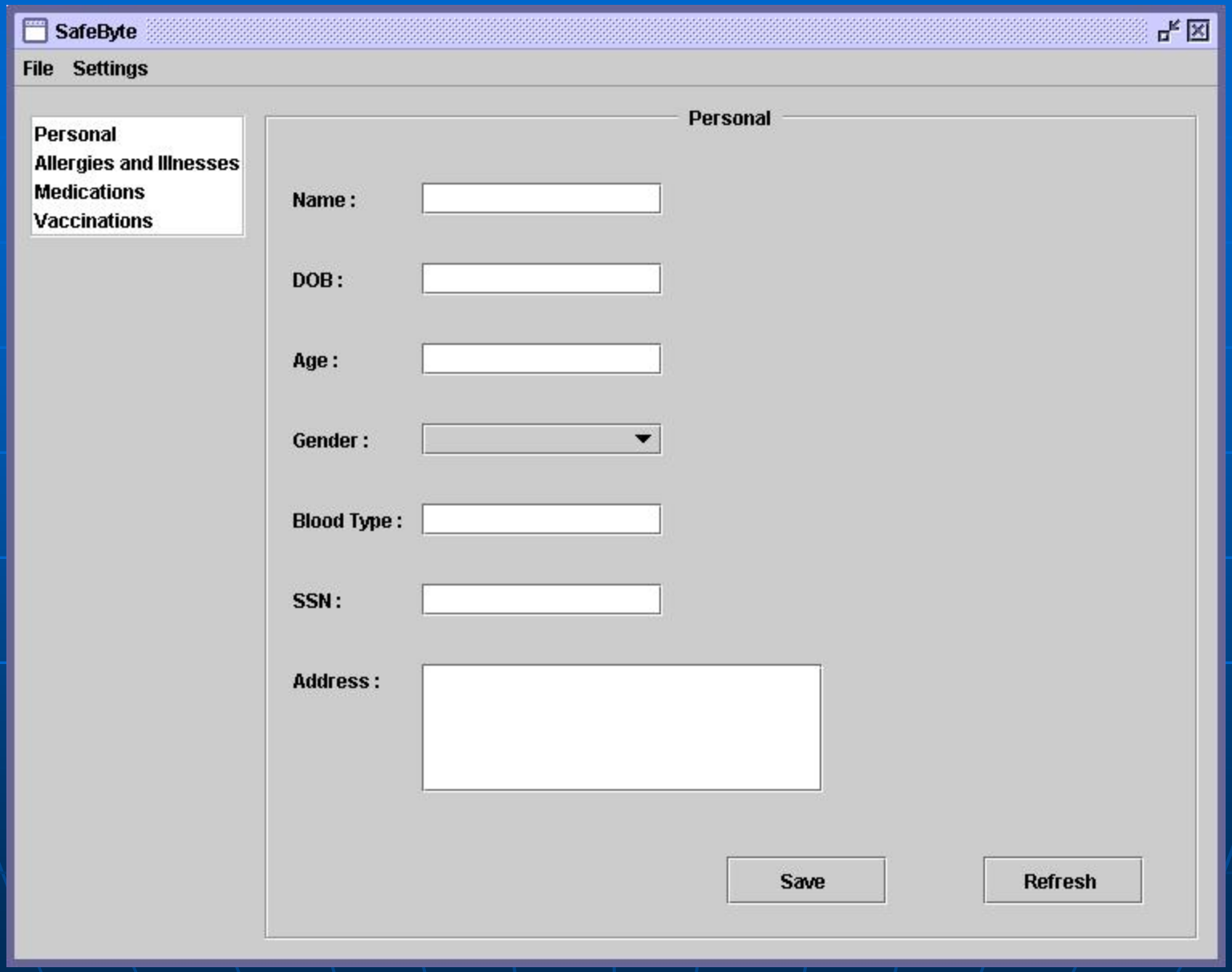
	Patients		Doctors		Pharmacists		Emergency
	See	Edit	See	Edit	See	Edit	See
Personal Information	X	X	X		X	X	X
Allergies and Illnesses	X	X	X	X	X	X	X
Medications	X		X	X	X	X	X
Vaccinations	X		X	X	X		

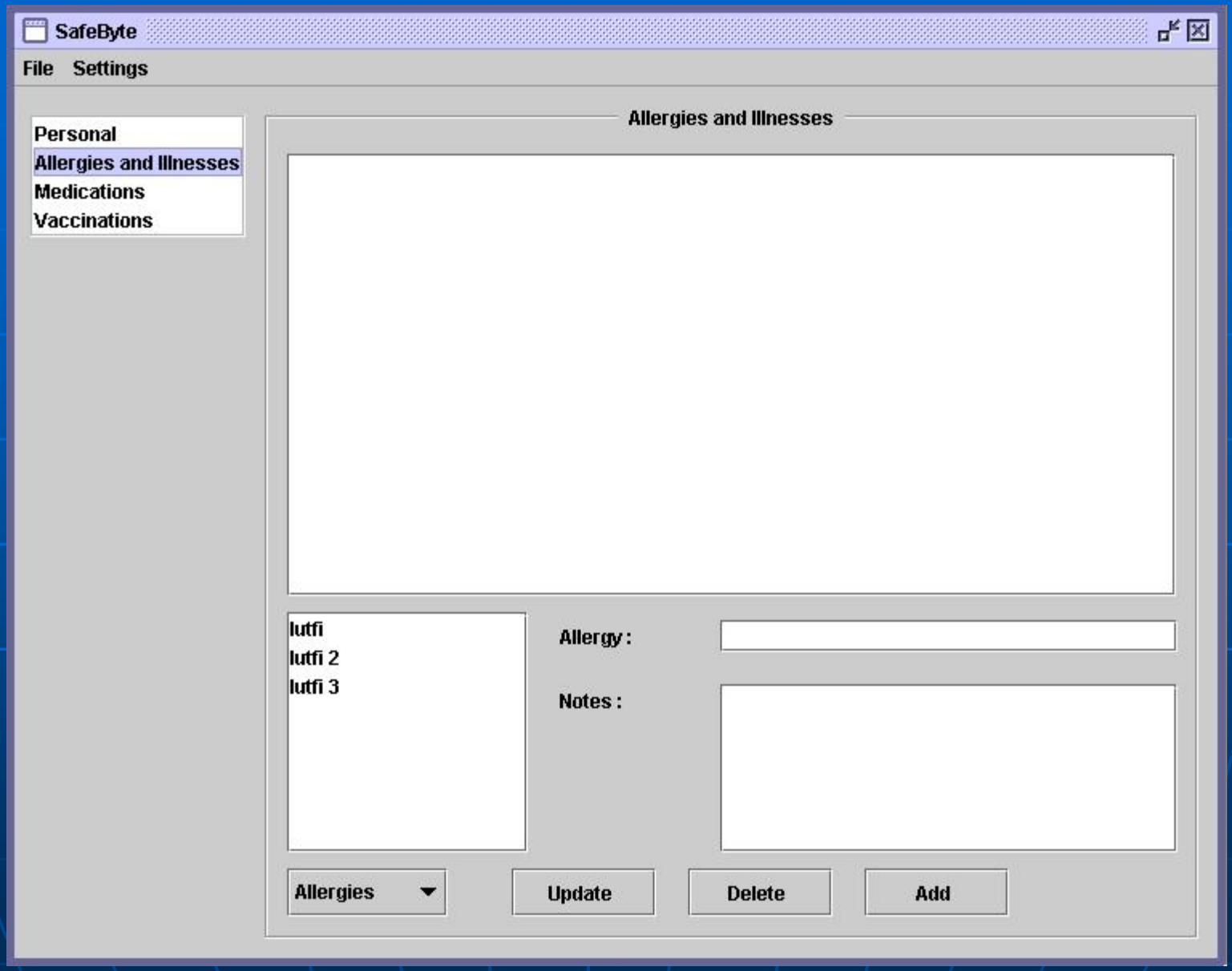

SafeByte - First Time Registeration
User Name :
Password :
Confirm Password :
Register

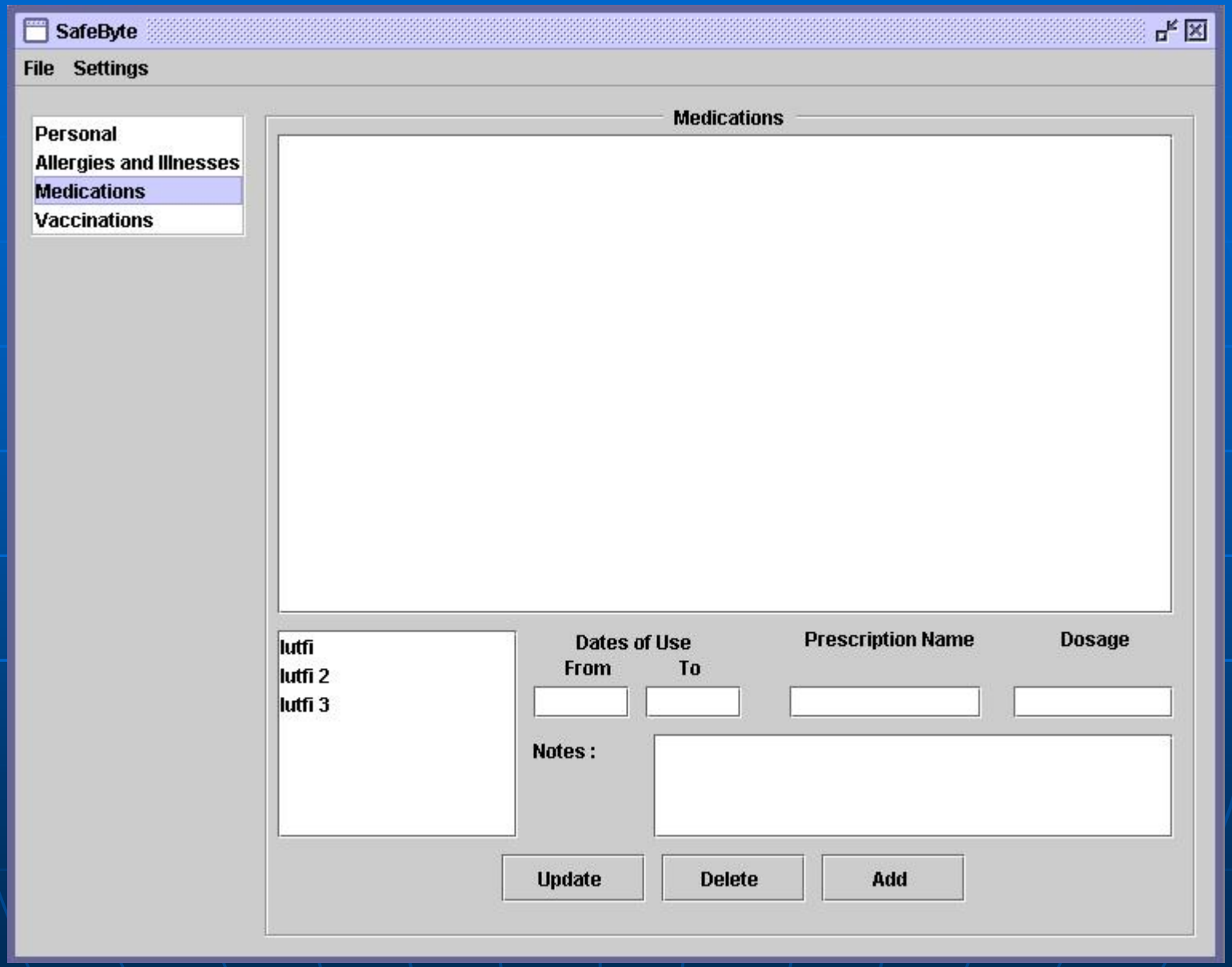

SafeByte - Log In
User Name :
Password :
Login
Emergency Information

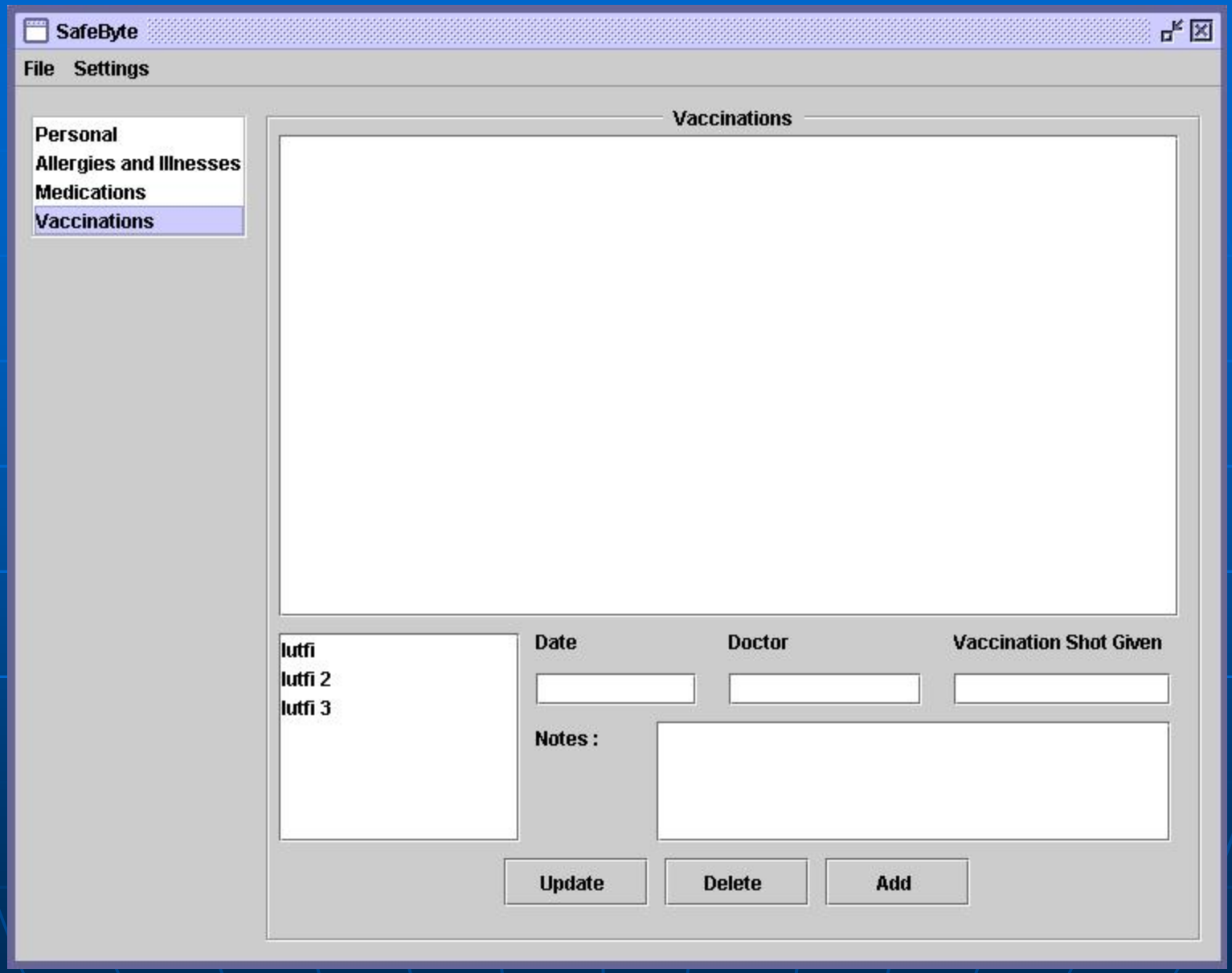

Emergency Information
Personal :
Lutfi Dughman
yadda yadda yadda

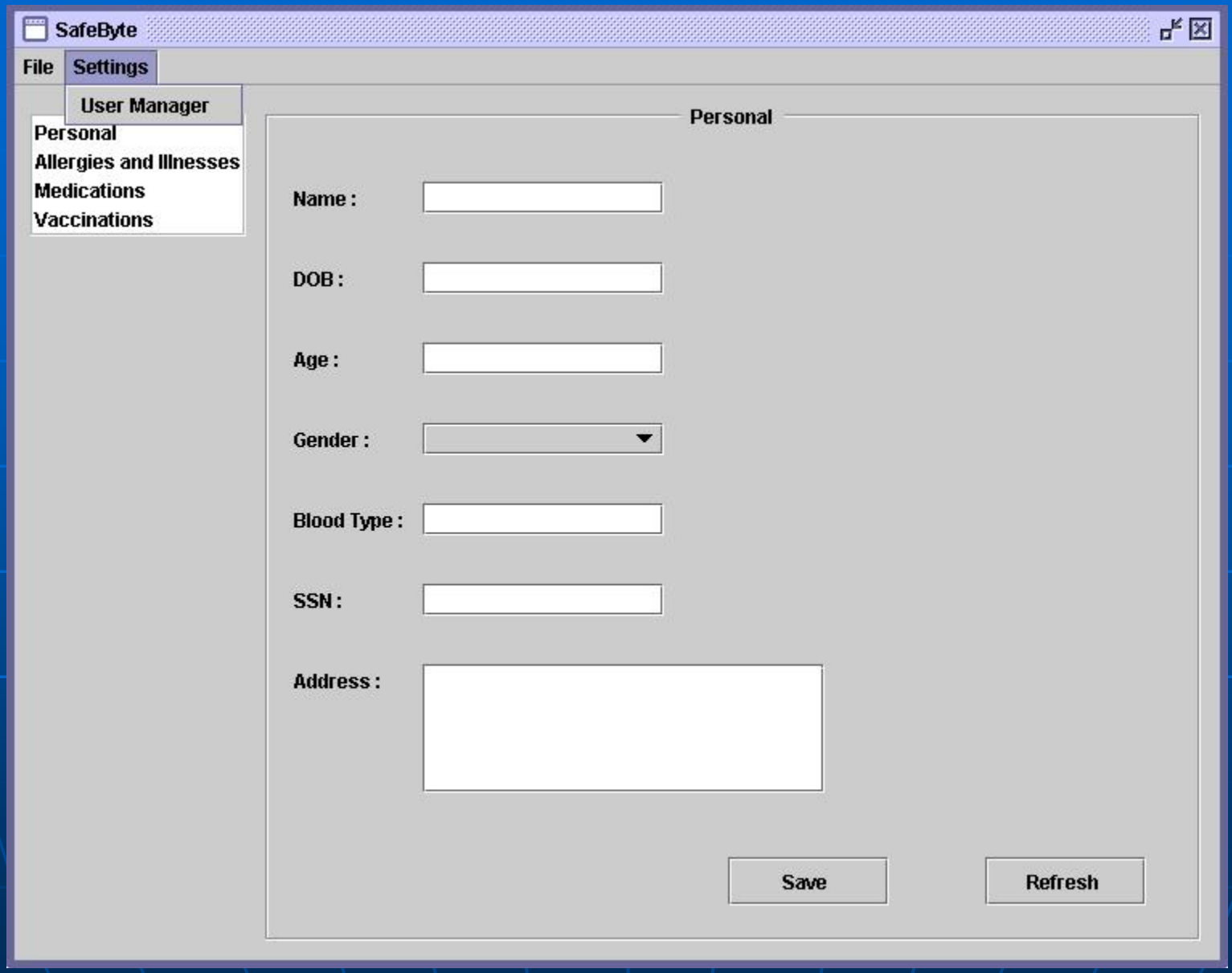
Back

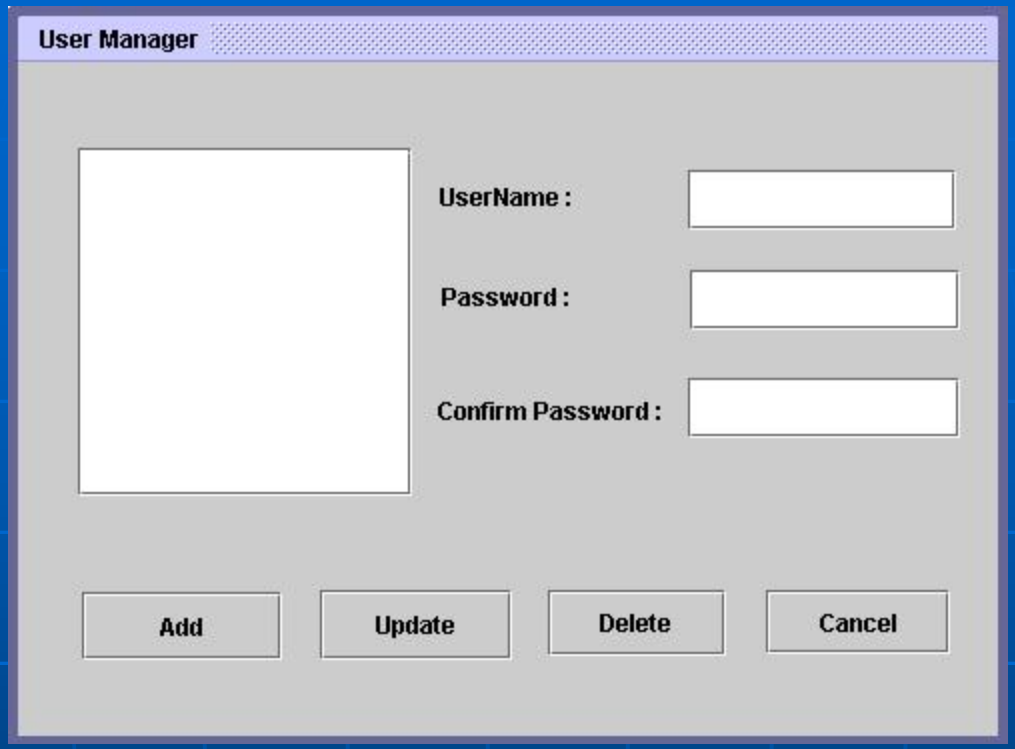

SafeByte
File
Settings
Personal
Allergies and Illnesses
Medications
Vaccinations
Personal
Name :
DOB :
Age :
Gender :
Blood Type :
SSN :
Address :
Save
Refresh


SafeByte
File
Settings
Personal
Allergies and Illnesses
Medications
Vaccinations
Allergies and Illnesses
lutfi
lutfi 2
lutfi 3
Allergy :
Notes :
Allergies
Update
Delete
Add


SafeByte
File
Settings
Personal
Allergies and Illnesses
Medications
Vaccinations
Medications
lutfi
lutfi 2
lutfi 3
Dates of Use
From
To
Prescription Name
Dosage
Notes :
Update
Delete
Add


SafeByte
File
Settings
Personal
Allergies and Illnesses
Medications
Vaccinations
Vaccinations
lutfi
lutfi 2
lutfi 3
Date
Doctor
Vaccination Shot Given
Notes :
Update
Delete
Add


SafeByte
File
Settings
User Manager
Personal
Allergies and Illnesses
Medications
Vaccinations
Personal
Name :
DOB :
Age :
Gender :
Blood Type :
SSN :
Address :
Save
Refresh


User Manager
UserName :
Password :
Confirm Password :
Add
Update
Delete
Cancel

Physical Interface Security

Physical Interface Security

Problem to Address:

- The flash drive must not have the ability to attack the host computer:
  - Disable the Autorun Feature in Windows
  - Identify the Correct Device for a Virus Scan

Physical Interface Security

Research:

- Identified Possible Flash Drive Threats
- Determined Solution Possibilities
- Chose the Most Feasible and Effective Solutions

Physical Interface Security

Solution:

Disabling Autorun

- Editing the Registry

Identifying Devices

- Device Scan
- Identification File
- Third Party Virus Scan

Physical Interface Security

2 of 3 Initial Layers of Defense:

- Autorun Prevention
  - Guarantees safety from a virus executing itself
- Virus Scan
  - Can ensure user that a virus is not embedded on the drive

Application Security:
Application Authentication Team

Why Authenticate SafeByte Software?

- Authentic software is important for any application that stores & manipulates a user's private information.

Unauthentic SafeByte Software can result from

- Viruses
- Hackers
- File errors

GOAL:
A practical way of checking if the SafeByte software is authentic….

Solution: Digital Signatures!

What is a Digital signature?

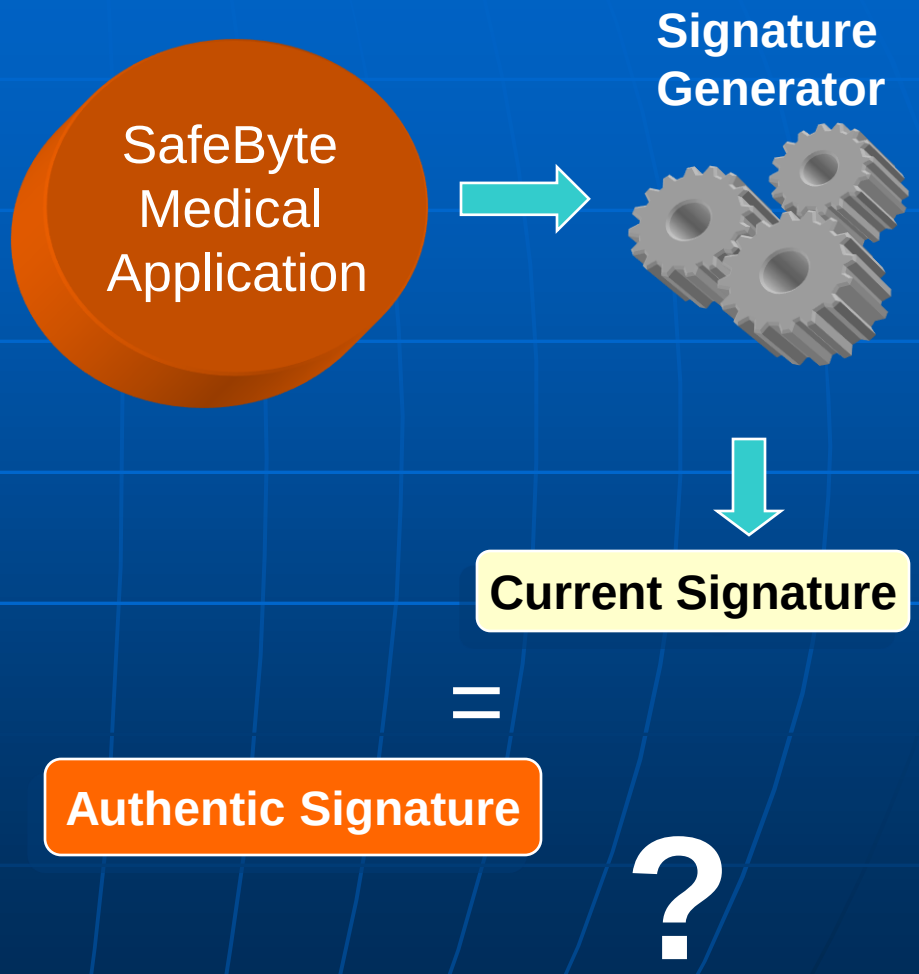
⇨ A Digital Signature is an electronic (digital) stamp or seal that is appended to data during data exchange.

How does it work?

- The slightest change to the SafeByte Medical Application will produce a very different signature
- Signatures are easy to use for comparison, as opposed to using the entire application

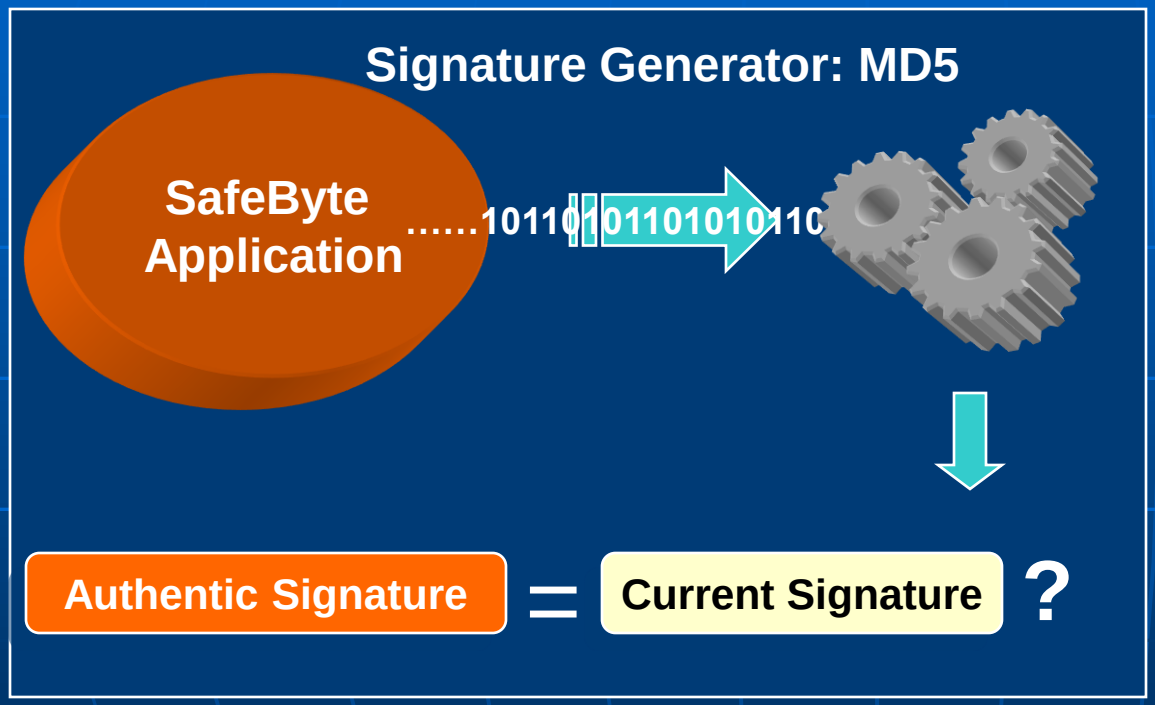
How SafeByte uses Digital Signatures:

- Authentic SafeByte software is passed through a signature generator
- The result is Authentic SafeByte Digital Signature
- Later on, another signature is generated by the user.
- The current SafeByte software is verified by comparing the current and authentic signatures.



Implementation

In Flash Drive…



MD5 algorithm.
MD5 can produce a unique 128 bit "digest" of an input of arbitrary length.

- True, then application is authentic.
- False, then application is not authentic, & not secure

THE FUTURE?!?!?!

- Will be able to verify the identities of Doctors, etc. using a third party source (internet)
- Will be able to store wider range of Medical Records

cybertrust

That's it !