

### The Challenge or problem

*How to allow doctors and other medical professionals to have access to patient medical records in emergency or other unexpected situations, when they do not normally have access rights to such records.*

It may not be feasible to request that access rights be given to the users at the time of access, due to time pressures or unavailability of the patient or administrator etc. We thus need an access control mechanism that can cater for these situations, by granting maximum freedom of access and, at the same time, maximum user responsibility for any exceptional actions taken.

Metaphor: "Breaking the glass" in an emergency situation to escape via a fire door.

### The Approach to address the Challenges

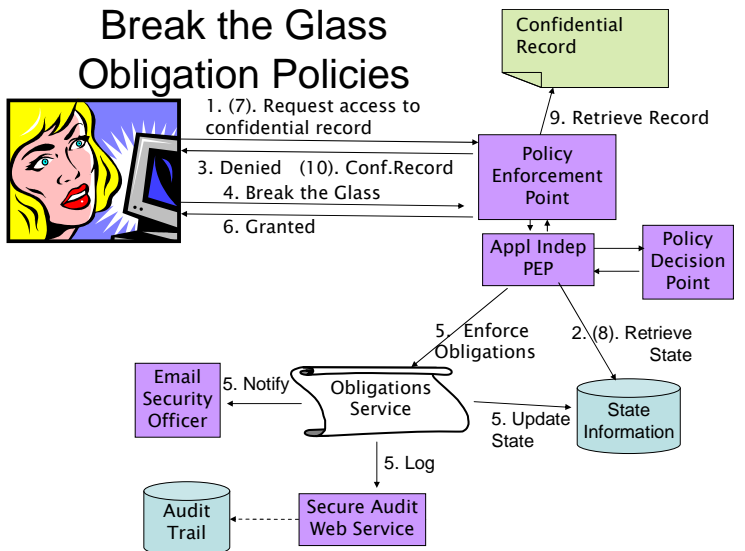
We define a new "break the glass" response to an access control decision request, to supplement the standard "grant" and "deny" responses. We define policy rules to specify when this new response should be returned. The new response means that the user is only allowed to access the resource if the user specifically takes responsibility for his/her actions. The application can respond to the user "You are not normally granted access to this resource, but you will be granted access if you decide to break the glass". The user can then choose whether to break the glass or not. If the user chooses to BTG, any application specific obligations in the policy will be enacted, such as: email the user's manager, record the access in a secure audit trail etc. The user will then be granted access to the resource.

We have implemented this using a standard policy decision point (PDP) and an application independent "break the glass" policy enforcement point which provides the enhanced level of functionality to the application. A public break the glass demonstration is available at

<http://issrg-testbed-2.cs.kent.ac.uk/>

### Primary interests

Application independent authorisation infrastructures.  
Privilege management. Identity management.  
Trust management. Privacy protection. Obligation Policies. Protection of Electronic Medical Records.



### Goals in attending workshop

1. Dissemination of our research results
2. Knowledge gathering
3. Determining new research opportunities
4. Networking with other attendees.

**For further information please contact:**

**Professor David Chadwick, Computing Laboratory,  
University of Kent, CT2 7NF  
[d.w.chadwick@kent.ac.uk](mailto:d.w.chadwick@kent.ac.uk)**