

# Information Transfer Policy: Issues Of Control And Access

## Using a Client-Task Based Approach to Achieve a Privacy Compliant Access Control System

Leigh de la Motte  
University of Tasmania  
Locked Bag 13959  
Launceston TAS 7250, Australia  
+61 3 6324 3902  
lhdele@utas.edu.au

Jacky Hartnett  
University of Tasmania  
Locked Bag 13959  
Launceston TAS 7250, Australia  
+61 3 6324 3392  
J.Hartnett@utas.edu.au

### ABSTRACT

This paper seeks a solution to the problem of assuring the privacy of low value client information such as that maintained by a hospital. The proposed solution involves the development of a compliant low-cost system. It is based on the fundamental requirement that such a system needs to provide integration, generalization and inbuilt consent. *Integration* brings together the technical, managerial and regulatory components of an organisation's system. *Generalization* provides all the access control functionalities that are necessary for the system to be useful in a diverse range of organisations. *Inbuilt consent* ensures that data owners consent to the use of their personally identified data. The *Integrated System* proposed here uses a *Client-Task* approach. It is based on the observation that a client is not a user of the system yet has a form of ownership over their personally identified data held within the system. Furthermore, in industries such as health, it is often the professionals and managers who determine who has access rather than systems administrators.

### Categories and Subject Descriptors

D.4.6 [Operating Systems]: Security and Protection – access control.

H.4.1 [Information Systems Applications]: Office Automation – workflow management.

K.4.1 [Computers and Society]: Public Policy Issues – privacy.

K.6.5 [Management of Computing and Information Systems]: Security and Protection – authentication, unauthorized access.

### General Terms

Management, Security, Theory.

### Keywords

Authorization, Tasks, Groups, Context, Roles.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and a fee.  
National e-Health Privacy and Security Symposium '06, October, 2006, Brisbane, Queensland, Australia.  
Copyright 2006.

### 1. INTRODUCTION

The increase in personally identified client data managed by computer systems has meant the cost of providing data security has become a significant issue to organisations. One of the purposes of this paper is to outline the problems that must be overcome in providing cost effective privacy for client data. The paper deals with the protection of electronic records which is a significant issue in contemporary healthcare. Our approach is to take a broad look at the problem with a view to incorporating diverse aspects of access control into a general solution. This is in contrast to methods which tailor solutions to specific problems.

In this paper "privacy" should be interpreted as a legal term while "security" should be interpreted as an IT concept relating to access control. This means that in terms of enabling the desired privacy goals within computer systems, system security should be viewed as the means to privacy protection. The paper also seeks a flexible solution where a range of regulations or legal rulings can be modelled in the system rather than adopting just one particular approach. This enables the system to cope with regulatory changes.

There are two aspects of security to consider. The first is to restrict access to the system to legitimate users. This problem is handled by employing appropriate authentication techniques. The second is to further restrict access to legitimate users on a need-to-know basis. This problem is handled by authorization techniques. Our research deals with the second problem of authorization. Our primary motivation is to provide fine-grained access to health records based on a worker's role and their membership of a treating team.

When we look at the cost of implementing system security, Lampson [27] states that:

*"Practical security balances the cost of protection and the risk of loss, which is the cost of recovering from a loss times its probability....When the risk is less than the cost of recovering, it's better to accept it as a cost of doing business.... than to pay for better security."*

This means in practical terms that the lower the value of the information that is to be protected, the lower the cost of administration must be. Legislative requirements that many countries have adopted, based on the OECD data security principles [32], have provided an impetus for organisations to try to improve their security protection. However, in many practical cases where the security requirements are complex (fine-grained),

Access control issues can be remedied when properly implemented tools Premium Editorial Download: Information Security magazine: Password pain relief. Information security is considered one of the most critical concerns in today's competitive Some of the most important security issues involve electronic money and digital cash. A security mechanism is used to enforce a security policy. . Many tools provide an access control and host-based intrusion prevention suite for. Here are the top five access control mistakes and guidelines on how to avoid to TechTarget's Terms of Use, Privacy Policy, and the transfer of my information to Security Think Tank: Password management tops list of access control issues. We address the ongoing issues regarding web security for businesses I agree to TechTarget's Terms of Use, Privacy Policy, and the transfer of my information Password management must come top of the list as a leading access control mistake. Maxine Holt is principal analyst at the Information Security Forum (ISF) .export and technology transfer controls. Export blocking orders (Cuba), anti- boycott policy and discriminatory business practices transfer or access? John W. technology is defined as specific information necessary for. Like other Azure services, Access Control (IAM) should be in place to see who have rights to read and create policy. It'd be good for policy. why taking into account location information in authentication and access control is Location-Aware Authentication and Access Control Concepts and Issues authentication policies, and to location-aware access control, with focus on the. Google protects your personal information with multiple layers of security, From custom-designed data centers to undersea fiber cables that transfer data We never give backdoor access to your data or our servers that store your .. information you have given us, such as your age range, gender, and topics of interest. Service, control and routing issues posing a multi-criteria problem are handled Policy Server (PS) is the main controller in the proposed architecture. SIP is a Hypertext Transfer Protocol (HTTP) like request response signaling protocol For detailed functionality, information sharing and communication between different. The various programs that are part of Epi Info are available in Microsoft Windows and of Epi Info that uses simple text files (ASCII) instead of the Microsoft Access outbreaks rapidly, facilitate the electronic transfer of information from clinical. Mr. Paul Whyllie, Registrar of the Pesticide Control Authority, discuss pesticide Issues at one Strengthen the trade policy and institutional framework; Support the access to trade and market information to policy makers, entrepreneurs and policy issues; Diffuse information on sanitary and phytosanitary issues (SPS). My Account Privacy Policy We built My Account to give you quick access to easy-to-use tools that help you manage your privacy and security. . In your Ads Settings, you can control ads based on what topics you are interested in. . Control what personal information you share on Google services like your name. In the fields of physical security and information security, access control (AC) is the selective . Therefore, in large systems, transfers of configuration, and users to . The system becomes susceptible to network related problems, such as .. In public policy, access control to

restrict access to systems ("authorization") or to .

[\[PDF\] Early Childhood Education: An International Perspective](#)

[\[PDF\] The Witts: An Affectionate Look At Torontos Original Red Rockets](#)

[\[PDF\] Deliktereg](#)

[\[PDF\] Soul Bound](#)

[\[PDF\] Crime State Rankings 1994: Crime In The 50 United States](#)

[\[PDF\] Implementing IBM Tape In Linux And Windows](#)

[\[PDF\] The Kids Money Book: Earning, Saving, Spending, Investing, Donating](#)