

Identity Management and the NHS

1 Introduction

1.1 The Identity Project Background

The Identity Project addressed the current practice and future needs of UK academic institutions in Identity Management ([IdM](#)). The [IdM](#) issues which were investigated included Grid use, Shibboleth installations of varying degree of maturity, collaborative courses and other long term inter-institutional collaborations, internal and shared dynamic virtual organisations, classes of users other than standard staff/student mix, library access schemes, and NHS involvement.

Partners in the project are:

- [Cardiff University](#) (project lead partner)
- [London School of Economics & Political Science](#) (leading the case studies work package)
- [Birkbeck College](#)
- [Goldsmiths College](#)
- [Imperial College London](#)
- [Queen Mary University of London](#)
- [Royal Holloway College](#)
- [School of Oriental & African Studies](#)
- [University College London](#)
- [University of London](#) (associate partner, not funded by the JISC)

Each partner carried out an audit of their [IdM](#) processes, as described in the [Audit final report](#). A large part of this was concerned with issues surrounding membership of an institution. The project also ran a wide-ranging survey, circulated to every HE institution in the UK, which also addressed these issues; this is described in the [Survey final report](#). This report is based on the information gathered through these activities.

The project started on 1 November 2006 and ended on 31 October 2007. The project was funded under the JISC [e-infrastructure programme](#).

Further information about the project generally can be found via the [project web site](#).

This report takes the information gained from the two major investigative work packages, the institutional audits and the survey, to obtain a picture across a range of institutions as to additional IDM practices necessary in an institution with NHS links. The primary focus of this report is on examining current IDM practice in force at institutions with NHS links – what extra burdens are placed upon an institution's IDM to handle the complexity that can exist in an institution with NHS staff, students, premises, and other links. This is an important area to investigate as many institutions do have links to the NHS, and this extra complexity is something that such institutions wishing to improve their IDM may need to consider.

2 Identity Management issues

Results from the survey and the audits have shown that having NHS links at in institution can cause several main issues to that institution's IDM. These are discussed in the following sections.

2.1 Membership issues

2.1.1 NHS links present extra members

An institution with NHS links may have many different extra categories of members that need to be dealt with by any IDM systems and procedures they may have. Generally, staff issues in this area seem more of an issue than students. Medical students of an institution are usually treated as students like any other, at least as far as membership issues are concerned, existing in the institution's Student Record System. Staff, however, are somewhat more complex. Four common examples of staff categories in existence are NHS staff who are also students at the institution, NHS staff who are contract holders of the institution, NHS staff who are honorary title holders at the institution, and NHS staff who teach students of the institution but have no formal affiliation with it. The Identity Project's IDM survey indicated that the former three categories were more prevalent at institutions than the latter, with some 70-80% indicating the presence of the former and 60% the latter. Other categories discovered are NHS staff who do collaborative research but do not have an formal affiliation with the institution and NHS staff who use library facilities (e.g. nurses and junior doctors).

This, of course, begs the question – why are these extra membership categories an issue? The answer to this question can be split into two main areas – legal and licensing issues, and technical issues.

2.1.2 Legal and licensing implications

Looking at the four categories of NHS related staff mentioned above, legally the first three categories should not present a problem – NHS staff who are students are therefore fully fledged students of the institution; NHS staff who hold a contract with the institution are fully fledged staff at the institution; NHS staff who hold an honorary title with the institution are fully fledged staff at the institution; however, the final category have no formal affiliation with the institution and therefore will not legally be counted as members of this.

Licenses that grant access to software or resources to “members” of the institution thus should not be used or accessed by such NHS staff with no formal institutional affiliation. However, in order to teach the institution's medical students, they may need access to such software or resources – e.g. they may need a computer on the institution's network to access the institution's VLE to add course material, and campus licenses for things such as Microsoft Windows and other software may not actually cover them; while they may need access to electronic resources licensed by an institution used as part of their course – the situation may occur where a member of NHS staff cites a paper from a medical journal that his students are allowed to access but that they are not!

See The Identity Project's separate report on membership issues for more information on general legal implications of membership issues.

2.1.3 Technical implications

An institution may wish such NHS/institution members as those mentioned above to access some of its resources and systems; for example access to its VLE to administer the courses that they teach, access to its email and/or collaborative tools, or one of many other things that would need a set of credentials (username/password) issued by the institution to gain access.

If an institution wishes its IDM system to provision and deprovision identities and these associated network/system account(s) in an automated way, then a data authority for that category of user should exist to provide the identity information necessary, such as name, job role (for assigning correct access rights), and start and end dates (for timely provisioning and deprovisioning), since these NHS/institution members may not exist in the institution's corporate systems (HR, Student

Records, etc). Such a data authority rarely exists in a form that can be directly linked to an advanced IDM system. It may exist, for example, in the form of one or more spreadsheets or databases administered by specific staff in an institution. Thus, such identity information would need to either be manually transcribed into an IDM system or manual extracts would need to flow between them and the IDM system.

One exception is that many NHS trusts contribute towards a database of NHS staff. This database is called Intrepid, and is administered by a company called HiCom². Some institutions take an extract from this and feed that into their IDM.

2.2 Separate networks

Many institutions with NHS links have a presence in NHS owned hospitals and other NHS buildings. Such NHS property typically has networking available for NHS computers connected to the NHS national networks (N3 in England and Scotland, DAWN2 in Wales). At some institutions, the institution's network also has a presence in the property, leading to the situation where a person may have two computers – one connected to each network – each with a different set of credentials used to log into the computer/network. One set of credentials would be the institution's network account, and one an NHS network account. At other institutions, the two networks are not present in the same buildings, but adjacent buildings, leading to the situation where a person may have to walk from one building to another in order to access resources on a particular network, again, having two sets of credentials.

This issue can be even more complex in medical schools shared between institutions. For example, in a joint medical school shared between two institutions, a person may have three sets of credentials – NHS credentials, and credentials for each institution!

2.3 Library access

Some institutions manage libraries used by both institutional and NHS staff members. This again has both legal and technical implications.

The legal implications are centred on whether such members of staff are entitled to access licensed resources (journals, e-journals, etc.). Such licenses may or may not allowed walk-in usage, and have specific definitions of what a “member” of the institution is. The recently published HAERVI report, commissioned by UCISA, explores this area in more detail.

Technical issues are more straightforward – if a person is to be allowed to borrow books from a library, they usually need an account in that institution's library management system. Thus, either there needs to be a data authority for that type of user to enable automatic provisioning of library accounts, or library staff will have to enter such staff members manually – potentially a large amount of work.

2.4 Access to electronic resources

A member with both an NHS affiliation and an institutional affiliation may have access to resources licensed by both. Gaining access to such resources would be typically via one of two methods – IP authenticated access or through the use of a Classic Athens account or through an institution's AthensDA² or Shibboleth service. Either way, the person would have two (or more in the case of joint medical schools) sets of credentials, each with its own set of resources. This can cause many issues such as the obvious problem of having to remember multiple username/passwords, having to remember which account can access which resources, potential cookie issues encountered when switching between accounts, etc.

In the case of at least one joint medical school, the medical school itself licenses particular medical

resources, and its members can access those as well as resources licensed to both institutions it is linked to, whereas members of those institutions can only access their own resources.

2.5 Physical Access

One final area of issue identified in the survey and IDM audits is that often an institution's premises may have physical access control systems (such as swipe or proximity card readers) to allow access to secure buildings and the NHS' premises would have a separate system. Thus, persons with the need to access both would have to be provisioned with two (or more) credentials (ID cards, swipe cards, etc), and have to carry both around.

3 Current institutional practise

The issues highlighted above are found in many institutions with NHS links. This section looks at how some institutions have made attempts at dealing with these issues.

3.1 Membership Issues

Some institutions have a firm grip on the membership problem, having devoted a fair amount of staff time auditing their membership, and making a decision about the affiliation and rights of each category. Drivers for this have included an institution having particularly complex partnership arrangements, and the use of Federated Access Management. Institutions are warned not to underestimate the time and effort required to complete this process.

Many institutions have overcome the problem of giving access to institutional resources to NHS staff without an official affiliation to the institution by giving them honorary titles, and thus becoming bona fide members of the institution. This is an approach that has worked well in many institutions. There are potential problems, however; an institution has to consider potential funding implications that may result because of the FTE and membership count increase these people with honorary titles may represent – software and/or resource licensing costs may increase accordingly. Also, some institution's procedures for gaining honorary titles may take a not-inconsiderable amount of time to happen. Having such new members not being able to gain access to resources for potentially a few months may be too long a time – especially in cases such as nurses on short courses, who may come and go in less than the amount of time the process takes.

3.2 Separate networks

In most, if not all, cases, the sets of credentials for the NHS network and the institutional network(s) are not connected in any way. Some institutions have tried to simplify life for its users by at least synchronising usernames by, for example, generating a set of username/passwords for its users and manually passing this list across to their NHS IT counterparts, who would create a set of NHS credentials with the same username. Thus, the person would still have two sets of credentials, but at the very least, only one username to remember (though, of course, passwords would not be automatically synchronised). While this approach does not solve any of the underlying problem, it does at least make life a little bit simpler for the relevant users. However, in some institutions, this has led to a practice where users are given their sets of credentials with the same username when they appear at the institution, and are then told to change the password on both accounts to be a new, identical password – and to never change it. While this makes life even easier for the user, it is obviously somewhat questionable security-wise!

Another solution in place at some institutions – though not a solution to the problem of multiple credentials, but rather to the problem of a person having to physically move to a different computer (or building!) to gain access to a resource on a particular network – is to implement a remote access

service such as that provided by Citrix which allows a user on one network to remotely connect to applications and/or resources available on the network hosting the service. Thus, for example, a person on the NHS network could connect (with appropriate permissions in place) to the institution's Citrix service and gain access to institutional applications and resources. This is often not a cheap solution, but it is a proven solution for this particular problem.

3.3 Library Access

See the HAERVI report, commissioned by UCISA, for an analysis of this area, including recommendations on how to improve the area.

3.4 Electronic Resources

Unfortunately, no easy or good solution to this problem exists. A pilot service allowing athens accounts to be linked together, giving the owner of the multiple accounts access to the full set of resources available to them was trialled, but institutions piloting the service reported to this project that it was too difficult to use from the perspective of their users.

Any solutions in this area are likely to be future developments enabled by new Federated Access Management technologies.

4 Conclusions

Institutions with links to the NHS may encounter several extra IDM issues that they may have to deal with. These centre around additional membership issues, the lack of data authority to provide an IDM system with identity information about NHS staff, the need to use NHS and institutional networks, library access, electronic resources, and physical access. Some institutions with such issues have enacted very similar solutions to the issues, however, many issues remain unsolved by all.