imprivata®

A Healthy Dose of Advice for Managing Clinician Access to Patient Data

Tips for Implementing SSO and Strong Authentication

You know your clinicians need faster access to patient data, and that accessing applications and searching for patient data is time consuming and frustrating for them. And, security requirements get in the way and cause disruption to their workflows. To address these issues, you need to eliminate password headaches and increase clinician satisfaction without negatively impacting patient data security.

The answer is single sign-on (SSO) and strong authentication (SA). But with resource constraints, tight budgets and the prospect of a disruptive organization-wide deployment, the idea of such an undertaking can be daunting.

At times like these, you need expert advice - not from a vendor, but from actual peers who have successfully deployed SSO and strong authentication at their hospitals - from those who have measured the results against the investment, and can share their experiences. So, we approached some of our healthcare customers and asked them what advice they'd give to other hospital IT executives who are contemplating the implementation of SSO and strong authentication. What follows are 20 valuable tips for successful procurement, implementation and deployment.

1. Perform due diligence to find the best form of strong authentication for each of your user groups.
Remember that different user groups have different requirements for access. Make sure that the solutions that you are considering are flexible enough to accommodate the access needs of all groups – today and down the road.

Dr. Stephen Patterson, Chief Medical Information Officer
H. Lee Moffitt Cancer Center - Tampa, Florida

2. Look for a tool that is appropriately sized for your organization.
SSO comes with lots of bells and whistles. Enterprise single sign-on solutions that integrate with your existing identity management systems -- in our case, Active Directory -- will save money and maintenance.

Chuck Christian, Chief Information Officer
Good Samaritan Hospital, Vincennes, Indiana

3. Understand how the solution(s) you choose work with technologies from other vendors.

Multiple vendors can and will work together if you push them. If integration is an important element of your project, bring it up early and don't move ahead without knowing that the vendor is committed to making it happen.

Joe Greene, CISSP, Information Security Operations Director
OhioHealth - Columbus, Ohio

Multiple vendors can and will work together if you push them.

4. Understand the workflow of your shared workstation departments.

If more than one person will be using a given workstation, you must validate that the SSO solution will not harm or break the existing workflow. Some SSO vendors handle fast-user-switching well, others do not. A quick—and clean—log-off can be as important as a quick logon. Find and work with your workforce experts. They will be a huge part of your success—if you enlist their help at the beginning.

Christopher Paidhrin, HIPAA and Security Officer,
ACS/Southwest Washington Medical Center, Vancouver, Washington

5. Engage your users early on.

Before you roll out - perhaps even before you have purchased - do a product demonstration for them. Odds are the users will be blown away with the simplicity of the authentication process and will clamber to sign up. In our case, it was the SSO and Strong Authentication solution that actually got the physicians excited about implementing the entire healthcare IT solution.

Bill McQuaid, AVP and CIO
Parkview Adventist Medical Center, Brunswick, Maine

6. Don't reinvent the wheel.

In many cases, you can take advantage of the technologies that you already have in place; for example, your proximity cards. Take an inventory of the technologies that your organization already owns and look for solutions that work well with your existing IT environment.

Michel Bouquet, IT Manager
Spaarne Ziekenhuis, Hoofddorp, Netherlands

7. Talk policy, not just machines.

Soft-peddling security policy does not work. I tell new employees that Big Brother "lives and breathes" at the medical center and the last person they want to see is me walking into their bosses' offices with audit logs.

Chuck Christian, Chief Information Officer
Good Samaritan Hospital, Vincennes, Indiana, Omaha, Nebraska

The nice thing about our solution is that it is architected in a way that is non-intrusive to the applications. That means that it never touches the application code or requires an agent on the server.

8. Consider your remote users.
If you have non-employees, remote contractors or partners, how will their provisioning be managed? Do you have one or more authentication data-stores (Active Directory, Novell, RADIUS, others)?

Christopher Paidhrin, HIPAA and Security Officer
ACS/Southwest Washington Medical Center, Vancouver, Washington

9. Write a user deployment plan and share it with your users.
Communication with users is critical to success. People are averse to change – even when it is for the better. Don't spring a new technology on them. Send email messages, hang posters communicating the benefits of SSO and SA. Let them know what's in it for them. Let them know that their workflow won't change.

Chuck Christian, Chief Information Officer,
Good Samaritan Hospital, Vincennes, Indiana

10. Develop a tightly managed internal security policy – before you deploy any authentication and access management solutions.
Though we are not bound by HIPAA, we feel that it is good practice to comply and follow guidelines where ever it makes sense. Our internal policies dictate that certain user access is limited to certain systems. Having our security policy defined and understanding the requirements helped us to come up with a deployment strategy to match that policy.

Michael Wilson, Infrastructure Director,
The Henry M. Jackson Foundation for the Advancement of Military Medicine, Inc. Rockville, Maryland

11. Do not over promise.
Once they have the convenience of SSO and strong authentication for access to critical applications, department heads will want every user enabled for every application. Stick to your plan and don't promise what you can't deliver.

Josh Rosales, Administrator, Security/Web/Backup/Network
Lake Forest Hospital, Lake Forest, IL

12. Know the cost of failure. If you have to remove the solution – for whatever reason, what is that going to require?
The nice thing about our solution is that it is architected in a way that is non-intrusive to the applications. That means that it never touches the application code or requires an agent on the server. This was reassuring for me as I could tell myself that if the solution didn't work out, I could just unplug the appliance. With other solutions I would have had to undo a lot of scripting, and the reworking could end up taking longer and costing more than the install.

Christopher Paidhrin, HIPAA and Security Officer
ACS/Southwest Washington Medical Center, Vancouver, Washington

13. Understand that no two departments (user groups) are the same.

Work with your "super users" well ahead of time. Help them to test, test and test. SSO is simple, but it is a change, and it ultimately affects everyone and everything. Identify unique users and PCs early on and have a plan for them.

Todor Yordanov, Systems Administrator or Director,
The Credit Valley Hospital, Mississauga, Ontario

SSO is simple, but it is a change, and it ultimately affects everyone and everything.

14. Make your users part of the process.

Seek their advice and learn their needs. We set up a physician steering committee to help guide our identity management strategy. It not only helped us to find the right product for our users' needs, but it helped us when the time came to roll out to the users. They were invested and ready to adopt the new system.

Dr. Michael Westcott, Chief Medical Information Officer
Alegent Health

15. Plan for auditing and reporting.

Know what types of audit and compliance reports will be required by your administration and be sure that your SSO solution can produce the appropriate results.

Christopher Paidhrin, HIPAA and Security Officer
ACS/Southwest Washington Medical Center, Vancouver, Washington

16. Determine where and how SSO should fit into your IT security strategy.

SSO is just one component of a complete identity management program. Yet it is one of the security features that we leverage in all the areas where equipment is used by multiple staff members, for multiple application access. The ability to easily lock a workstation and have all the applications protected is a real plus and requirement.

Chuck Christian, Chief Information Officer
Good Samaritan Hospital, Vincennes, Indiana

17. Think like a user.

Before you deploy, put yourself in your users' shoes and do everything you can to try to break the system. Then test, test, and test. You only have one chance to make a first impression with your doctors and nurses.

Bill McQuaid, AVP and CIO
Parkview Adventist Medical Center, Brunswick, Maine

imprivata®

About Imprivata

Imprivata is a leading provider of authentication and access management solutions for the healthcare industry. Imprivata's Single Sign-On and Authentication Management enable fast, secure and more efficient access to healthcare information technology systems to address multiple security challenges and improve provider productivity for better focus on patient care. Over 2 million care providers in more than 1,000 healthcare organizations worldwide rely on Imprivata solutions.

For further information
please contact us at:
+44 (0)208 744 6500
or visit us online at
www.imprivata.co.uk

Offices in:
Uxbridge, UK
Lexington, MA USA
San Fransisco, CA USA
Santa Cruz, CA USA
Paris, France
Nuremberg, Germany
Den Haag, Netherlands

18. Ask which strong authentication methods the products support directly.

Even if you have already decided on a method for today, user requirements and technologies are apt to change, the price of devices can decrease, and you want to be sure that you have choices down the road. Also ask if strong authentication methods can be mixed and matched for different user groups.

Mike Mitchell, Network and Applications Analyst
William Osler Health Centre, Brampton, Ontario

19. Keep it simple.

For organizations whose staff log on to multiple workstations during the day, keeping the look and feel of SSO solutions the same is important. It is important to cut down on confusion.

Chuck Christian, Chief Information Officer
Good Samaritan Hospital, Vincennes, Indiana

20. Have a back-up plan.

I enroll all ten fingers for each user. That way if a doctor or nurse has a cut or burn on their primary finger, they can move to another. As a last resort, all my users can fall back on a password. So far, we have not had any issues, but I can't take the risk of having a clinician locked out.

Bill McQuaid, AVP and CIO
Parkview Adventist Medical Center, Brunswick, Maine

WP-Healthy Dose-UK-Ver1-0515