Quick and secure access to patients' data – Statutory requirements and solution approaches

Healthcare institutions depend on secure and efficient workflows. The demands for data protection and productivity can be reconciled perfectly with a combination of single sign-on, authentication management and thin clients.

Contents:

- The requirement: valid information round the clock
- The risk: current threats to data protection
- The law: what regulations must be observed?
- The tradition: what existing approaches are there?
- The future: what does a state-of-the-art solution look like?
- The implementation: IGEL thin/zero clients and Imprivata single sign-on and authentication management

imprivata®

IGEL® TECHNOLOGY

The way in which companies and government agencies provide their IT has been undergoing huge changes for a number of years now. With the help of virtualization, applications and desktops can be bundled together in the computer center and provided locally with never-before-seen efficiency. At the same time, there is the possibility of comprehensively outsourcing l Valid information and rapid access to it are vital in providing medical treatment. Surgeons need precise X-rays, internists require laboratory data to administer the right medication, and the emergency department must have blood type data as soon as a patient is admitted. To keep on improving medical care, the patient's medical record must be able to be read at the crucial moment and access to data must be available round the clock. A hospital's administration department also relies on precise and valid data for its tasks, which range from order management, procurement, logistics and cleaning to billing.

Risks from unauthorized access to the HIS

To enable all that, hospital information systems (HISs) provide a large number of data records from a wide range of different sources. Extensive medical records are intended to help identify promising ways of treating hospital patients. Yet technical progress also brings risks with it. If the HIS is not protected against unauthorized queries relating to personal health data or if access to databases cannot be adequately logged, the hospital may face serious compliance problems. An example:

> The nurse Bernard K. wants to find out about the state of health of his neighbor, who is in intensive care. To do that, he logs on to the HIS using the password of the chief physician for urology. Bernard K. gleaned it from a post-it stuck to a computer in the urology ward. He searches the database for urology patients and discovers his neighbor has prostate cancer.

This case example shows how carelessness in the use of passwords jeopardizes data protection and patients' privacy. And the damage is even greater if passwords are deliberately misused by people who manipulate patients' data under a false name.

Password management as a vicious circle

Although the German Federal Office for Information Security (BSI) provides helpful information on appropriate ways to create, organize and use passwords[1], German data protection authorities repeatedly criticize deficiencies in everyday practice[2]: Passwords are written on bits of paper and stuck to the computer or comprise (solely) the user's name. In view of the fact that staff are under time pressure, circumventing the password guidelines is certainly understandable. They don't want to spend a lot of time trying to recall their password or complete time-consuming identification processes, especially given that they usually have to remember several passwords for different wards and IT applications. If IT administrators respond to such lax security by introducing a limited period of validity for passwords or stricter requirements for their complexity, employees' willingness to cooperate diminishes further. The result is a vicious circle.

PRINCIPLES OF DATA PROTECTION LAW FOR HOSPITALS RUN BY ALL ORGANIZATIONS:

- Collection, processing or use of personal data is permissible under data protection legislation only if it is permitted by a statutory provision or is done with the data subject's consent[6]. Any transfer of personal data must be authorized by a statutory provision or under a valid declaration of consent under data protection law.
- Medical data is a special kind of personal data[7] and so is subject to special regulations.
- Persons or institutions that use personal data must take suitable technical and organizational measures. In its Annex to Section 9, first sentence, the BDSG specifies measures such as:
  - Preventing unauthorized persons from using data processing (DP) systems (access control, No. 2), for example by deactivating the screen after a specific period of inactivity[8] (disadvantage: work is interrupted if the password has to be entered repeatedly)
  - Restricting use of DP systems solely to the data the user is authorized to access, and protection of personal data during processing and use and after it has been stored against being read, copied, altered or removed without authorization (access control, No. 3)
  - Ensuring that it is possible after the fact to identify the user who has entered personal data into, altered it or removed it from data processing systems (input control, No. 5)

Differing statutory regulations…

There are now pretty clear regulations that must be heeded to protect patients' and medical data. First, there is the obligation of medical confidentiality enshrined in legislation governing the medical profession, flanked by German criminal law (Section 203 of the German Penal Code (StGB)). This stipulates that medical professionals must maintain secrecy on what has been confided to them or on what they have gained knowledge of in their capacity as a physician[3]. Although this obligation is directly incumbent on doctors and their assistants, it indirectly affects the work of hospitals, which after all are responsible as employers for their personnel.

There are also regulations for protecting personal medical data, which differ depending on who runs the institution. The German Federal Data Protection Act (BDSG) applies to privately run hospitals, while those run by the federal states are governed by the respective state's data protection laws and/or more specific data privacy regulations under state hospital legislation. Church-run hospitals are subject to data privacy regulations of the church in question.

… with a consistent tenor

These regulations have one thing in common: They all embody the same principles of data protection law (see box 1). As regards hospital information systems, the German data protection authorities especially focus their supervisory activities on ensuring that patients' data is not allowed to be seen by all hospital staff, but only as and when actually required on the basis of the person's particular role[4], for example as a doctor on a specific ward[5]. That means permission to access patients' personal data is dependent on the specific role of each hospital employee.

Risks in traditional solution approaches

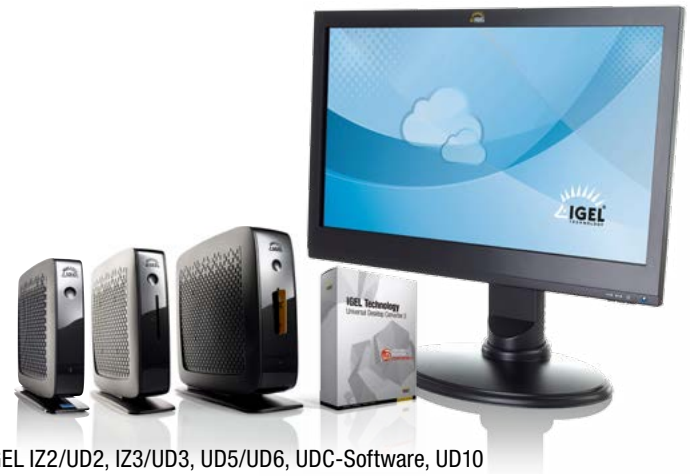
In order to meet these requirements in compliance with the regulations, many institutions have introduced single sign-on[9] (SSO) procedures for the various DP systems or places of work. Whilst SSO reduces the number of logins somewhat, if health professionals change ward frequently, their DP systems will be closed each time, forcing them to restart their desktop dozens of times during a single shift. As a result, a busy shift may mean that the documentation remains incomplete and so result in cases of liability.

Another typical compliance approach is based on the use of passwords that are assigned either to a specific user name or – as in two-factor authentication – to a means of identification, such as a smart card or token.

However, a critical aspect is that both have the disadvantage that repeated logging on and off disrupts the work and concentration of hospital staff. So that time can be gained for looking after patients, practices that are problematic from the data protection point of view have often become established, such as one password for the whole department or leaving work sessions open. If hospitals follow these traditional approaches, they risk compromising the quality of medical care, as well as missing their financial targets. If violations of the law are even tolerated in practice, the hospital faces fines, criminal penalties and ultimately a loss of trust among patients, health insurers and public authorities.

A harmonious balance between compliance and usability

State-of-the-art solutions eliminate these risks by minimizing the number of times passwords have to be entered either by means of a single sign-on approach for multiple systems or making input of a password superfluous with the aid of authentication management. In particular, the provider Imprivata has made a name for itself worldwide with such features. In order to optimize workflows, the single sign-on solution from Imprivata automates input of user names and passwords for authorized users, independently of the Active Directory (AD).

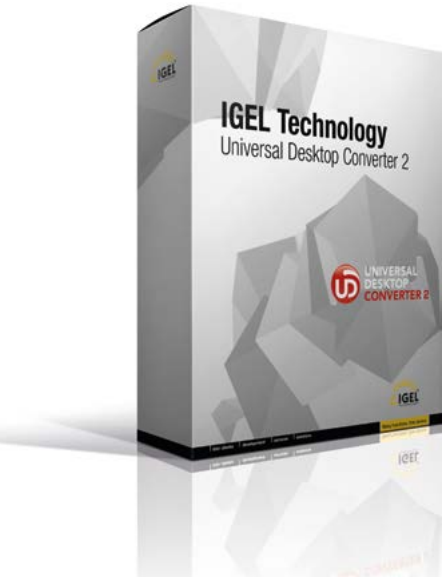


IGEL IZ2/UD2, IZ3/UD3, UD5/UD6, UDC-Software, UD10

In combination with optional authentication management, staff also obtain No-Click Access™ to desktops and applications. Instead of a lot of mouse clicks, all users need to do to log on to the HIS is to have their ID badge or fingerprint read. Additionally, the walk-away security feature prevents unauthorized access: The screen automatically fades and the workstation is locked after it has been used. The Self-Service Password Management function from Imprivata also saves further time and money, since it enables users to reset or change their passwords securely and without the need to get in touch with a help desk.

Further gains in efficiency thanks to thin clients

Since most hospitals have a central IT infrastructure, combining Imprivata's solutions with thin clients is a persuasive means of enhancing efficiency. According to a recent study by the Fraunhofer Institute UMSICHT, the total cost of ownership of 100 thin clients over a period of three years was up to 55 percent lower than that in a scenario with 100 PCs[10]. The savings rose as the number of users and length of time increased. In view of these synergy effects, Imprivata has a technology partnership with the German market leader IGEL Technology. Its thin and zero clients work together with various virtualization solutions, above all Citrix XenApp / XenDesktop, Microsoft RDS and VMware Horizon. Thanks to seamless integration with Imprivata, IGEL's users benefit from additional improvements in workflows. For instance, the their personal desktop goes wherever they go (follow-me desktop). When users are (automatically) logged off from a thin client and log on again to another, they see the exact same content on the screen as in their last session.



IGEL UNIVERSAL DESKTOP CONVERTER 2 (UDC2): HOW SOFTWARE THIN CLIENTS HELP CUT COSTS:

- Low capital expense: no hardware costs for thin/zero clients
- Immediately frees up funds in the IT budget, which can be used for other investments
- Efficient, secure and site-independent remote administration of the devices
- Cost-efficient setup of mobile thin clients
- Uniform management of all IGEL devices and converted hardware (software thin clients)
- Dramatic reduction in administration costs
- Longer operation of new and existing hardware
- The solution can be updated (e.g. with Citrix Receiver) and so is future-proof
- Standardized user interface in hybrid PC and thin client infrastructures

imprivata®

demo video from Imprivata:

IGEL and Imprivata – A veritable solution

The two partners – IGEL and Imprivata – are regarded as a firm force in the healthcare sector. More than half of German hospitals set store by thin and zero clients from IGEL, while Imprivata can cite more than 1,300 references worldwide. A combination of both solutions allows institutions to leverage the efficiency advantages of modern IT concepts, such as a virtual desktop infrastructure (VDI). That enables users to gain immediate access to their virtual desktop without a single mouse click using an energy-efficient thin or zero client. To achieve maximum cost-effectiveness, both Imprivata and IGEL thin and zero clients can be implemented and remotely administered by means of an easy-to-use graphical interface – without the need for scripting. The complete remote management solution with the title IGEL Universal Management Suite (UMS) comes with all thin and zero clients. The vendor's product portfolio also includes software thin clients, logical thin clients that are generated on the existing PC hardware through installation of the lean operating system IGEL Universal Desktop Converter 2 (UDC2). That means investments in new hardware can be avoided if required and funds from the IT budget freed up and put to other use – for example for an efficient single sign-on solution like Imprivata.

High availability of the IT base

A further interesting application scenario is mobile thin clients, which can likewise be generated on x86-compatible notebook hardware with the aid of the thin client software IGEL UDC2. Mobile IGEL thin clients are also compatible with Imprivata and the IGEL UMS remote management solution. The maintenance costs for this client hardware tend toward zero, since they no longer have to be repaired and no local data has to be saved. If the hardware fails, the IT team configures a replacement device in the space of minutes by assigning a profile in the UMS console. Practical features for modern hospital operations which IGEL supports are not only the obligatory health card readers, but also touchscreens with resolutions of up to 2560 x 1600 pixels and market-leading digital dictation solutions. IGEL offers an extended warranty of up to five years for its multi-protocol thin clients, which run without a fan and so are suitable for use in operating theaters even without an additional housing.

SECURITY IN A LEAN SOLUTION: BENEFITS FROM IGEL THIN CLIENTS FOR IMPRIVATA CUSTOMERS:

- Simple data access thanks to touchscreen support
- More security in mobile working (log-on and data access)
- Digital dictation with market-leading solutions from Grundig, Philips and Olympus, etc.
- Support of the electronic health card (eHC)
- 24/7 operation thanks to stable, low-maintenance systems
- No air or germ circulation thanks to fanless (silent) hardware
- Diverse connectivity options: USB, serial, parallel, and WLAN (optional); even compatible with older peripherals and fiber optic network cards
- High screen resolutions (up to 2560 x 1600 pixels)

VORTEILE EINER KOMBINIERTEN LÖSUNG AUS IGEL THIN CLIENTS UND IMPRIVATA:

- Provides fast, uncomplicated access to virtual desktops – with No-Click Access™
- Allows secure authentication by means of an ID proximity badge, a smart card or fingerprint
- Works with all types of clinical, financial and administrative applications
- Fewer calls to the help desk thanks to password self service
- Compliant, enhanced workflows for doctors, nurses, administration and IT
- Use of virtual desktop infrastructures: Citrix XenDesktop / XenApp, VMware Horizon, Microsoft App-V and Microsoft RDS
- Possibility of gentle migration by continued operation of older PCs as software thin clients (IGEL UDC2)

Conclusion

A combination of IGEL thin clients and the Imprivata SSO solution with authentication management enables hospitals and clinics to reconcile the two apparently conflicting objectives of compliance and productivity and achieve permanent cost savings. As a result, data protection, productivity and IT efficiency can be squared – producing very great benefits in the shape of lean workflows and an ideal quality of care. **T operations as a service as part of XaaS[1]. Regardless of whether companies provide their services via a self-managed private cloud or using a hybrid cloud with their own and external IT services, the traditional, high-maintenance workstation PC is no longer required. At modern workstations, PCs which date back to the 1980s and are also referred to as "fat clients" owing to their extensive hardware are being replaced by a thin or zero client with standardized remote management in order to further increase the cost saving potential of cloud computing.**

[1] German Federal Office for Information Security (BSI), IT Baseline Protection Catalogs, Catalogs of Measures, M 2.11 Regulations on Password Use [2] See, for example, the Data Protection Commissioner of Baden-Württemberg, Information, Use of Passwords, dated June 25, 2010 [3] Cf. Section 9 of the Model Professional Code for Physicians in Germany (MBO-Ä) [4] Decision by the 81st Conference of National and State Data Protection Commissioners in Würzburg on March 16/17, 2011: "Guidance on Hospital Information Systems" [5] Cf. No. 13 Key Normative Points in the Guidance on Hospital Information Systems [6] Cf. Section 4 (1) BDSG, for example [7] Cf. Section 3 (9) BDSG, for example [8] German Federal Office for Information Security (BSI), IT Baseline Protection Catalogs, Catalogs of Measures, M 2.11 Screen Lock [9] Single sign-on means that users can authenticate themselves once only at a workplace and then have access to all computers and services they have local authorization for at the same place of work, without having to log on again each time. If users change their place of work, the authentication and local authorization are no longer valid. [10] Study by the Fraunhofer Institute UMSICHT "Ecological and Economic Aspects of Software Thin Clients" (short title: Thin Clients 2015): "[…] the costs for the desktop PC in a scenario with 100 clients were around €2,165 and around €2,590 for the notebook. In contrast, the estimated costs for an older desktop PC operated as a logical thin client are around €1,157, for a notebook run as a logical thin client around €1,176 and for the hardware thin client €1,413."

IGEL Technology America, LLC | info@igelamerica.com | www.igel.com/us

GERMANY Augsburg, Bremen, Mainz | **AUSTRALIA** Sydney | **AUSTRIA** Vienna | **BELGIUM** Leuven | **CHINA** Beijing, Shanghai | **FRANCE** Paris | **THE NETHERLANDS** Utrecht | **SWEDEN** Vänersborg | **SWITZERLAND** Zurich | **UNITED KINGDOM** Reading | **UNITED STATES** Cincinnati, New York