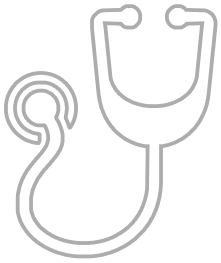
SAFEND DPS FOR HEALTHCARE

Whitepaper



safend
a SuperCom company

WHY NOT PROTECTING SENSITIVE DATA PUTS YOUR HEALTHCARE FACILITY AT RISK

Changing the face of healthcare, today's communication technologies bring new risks and challenges related to data, its sensitivity, usage and security. While protecting sensitive information, these changes have introduced stringent regulations and standards like GDPR EU, which bring additional demands on healthcare facilities. When looking at data-protection solutions, a major requirement is to define sensitive information, learn about data theft risks and understand their effect on your facility.

What is sensitive information at healthcare facilities?

- Personal information about patients
- Personal information about staff
- Patient medical history
- Patient and staff financial history
- Healthcare facility management information

Main data theft risks at healthcare facilities

- Internal data theft, either intentional or unintentional
- Leakage of sensitive data via endpoints: ports and USB storage devices, external devices like CDs, DVDs and printers
- Unauthorized access of unprotected data
- Unauthorized access of protected data
- Sending classified information to the wrong recipient

How can these risks effect a healthcare facility?

- Legal actions by patients or their representatives following misuse of their sensitive information
- Potential fines after failing to comply with local standards or to report a successful cyber-attack
- Loss of integrity and reputation
- Problematic patient and staff retention
- Loss of manpower and work hours when handling patient complaints
- Heavy financial losses resulting from successful data theft activities

WHAT ARE THE DATA-PROTECTION CHALLENGES?

Providing a strong technological solution to data-protection and remaining compliant to required regulations and standards without effecting end-user efficiency.
Additional major challenges include ways to control access to sensitive data files and folders, data encryption and how and where information is saved and downloaded to. The use of external devices and remaining alert and in the loop by continual analysis of the solution's services are also integral requirements.

Remaining updated with compliancy standards like GDPR EU

- Understanding and complying with local and international standards
- Understanding and complying with standards in countries you do business with.

Where is sensitive data most open to threat?

- Endpoints on computers, laptops and mobile devices
- External media like USB storage sticks, CDs and DVDs
- During its transfer

A few facts and figures for 2016

- Texas-based Integrity Transitional Hospital: lab results of 29,514 patients were compromised.
- New Mexico Hospital, Albuquerque: technical issue with hospital billing systems caused medical information of over 2,800 patients to be mailed to incorrect addresses
- UnityPoint Health-Allen Hospital, Iowa: data breach stealing personal information including social security numbers of 1,620 people
- Keck Medicin, Los Angeles: data files on two servers were made inaccessible to employees after being compromised with Ransomware. The hospital did not pay the ransom money

Knowing where sensitive data is at all times

- Defining strong access permissions
- Preventing good people from doing bad things
- Preventing bad people from doing bad things

How to prevent stolen data from being used

- Defining which information can be uploaded to where
- Encrypting sensitive information

HOW SAFEND DPS ANSWERS DATA PROTECTION DILEMAS

Silent operation without disrupting daily activities

The Safend DPS Data Protection for Healthcare solution is based on the Protector, Encryptor and Auditor modules which balance between productivity and performance without interfering with daily work activities.

When installing DPS onto a network, accurate analysis of data protection requirements are assessed. This enables building policies and their exceptions, profiling and adding user / machine permissions also regarding the use of USB storage drives and other external storage devices.

As a granular suite, monitoring and controlling the information flow on your facility endpoints, DPS enforces these policies, permissions and exceptions as it protects, encrypts, audits and generates reports on use of ports and devices. For example, when uploading an Excel file to a CD - an external device - which is an exception to a policy blocking use of all external devices.

Cost-efficiency, leaving room for future growth

Integrating Safend DPS into your facility's data network helps side-step costs associated with data leakage through unprotected endpoints. Safend DPS currently has the capacity to support over 250,000 endpoints via one environment.

Understanding compliancy requirements

Safend DPS already meets EU GDPR standards and as a customizable solution, can make necessary provisions should modifications be required. DPS also answers additional major compliance requirements like SOX, HIPAA, PCI, FISMA, BASEL II, UK Data Protection Act (DPA) and other stringent standards.

Overcoming integration pains

Safend DPS is designed for comprehensive installation and can be installed by both Safend certified experts or by your facility's system administrator. Depending on the solution's requirements, the entire integration process should take a short time.

Safend DPS profiles, policies and exceptions

Prior to server installation, DPS can pinpoint the usage of USB, FireWire, PCMCIA, PCI, internal storage and WiFi connections at your facility. Using this information provides administrators the knowledge they need to create enforced preventative policies, permissions and exceptions.

This may include blocking all external devices and then assigning exceptions to different users / devices, or that specific information only can be uploaded to an external device.

More facts and figures

- Vista Research: 70% of data leakage originates from within an enterprise
- Forrester: 52% large North American enterprises lost confidential data through removable media like USB drives
- IDC: over 60% confidential data resides on endpoints
- Ponemon Institute: over 16,000 laptops are lost each week by in-transit business men and women in USA, Europe and UAE

Safend DPS offers the following options:

- Blocking / enabling data transfer
- Blocking data transfer and collecting information
- Blocking data transfer without collecting information
- Enabling data transfer and collecting information
- Enabling data transfer without collecting information

One Data Protection Suite, One Data Protection Agent

Built as a suite of data protection modules, DPS protects your information as it controls, encrypts, monitors and updates you about its whereabouts throughout its lifecycle.

Safend Data Protection Suite Modules

- Protector: controlled port and device endpoints and media encryption
- Encryptor: transparent encryption on laptops and PCs
- Auditor: immediate risk detection on WiFi ports / devices connected to endpoints

Protector, port and device endpoints control

A flexible and intuitive solution with strong rule-based file encryption capabilities, Protector averts inappropriate use of smartphones, digital cameras or memory sticks. Protector enables creation of highly granular and customizable security policies which automatically detect, permit and restrict files and selected devices according to levelled user permissions, type, model and serial number.

Encryptor, full data hard disk encryption

A full encryption solution for healthcare information, Encryptor blocks inappropriate access or transfer of information. As it secures a facility's endpoints, Encryptor immediately alerts administration on all intentional / unintentional data leakage incidents.

Always one step ahead of existing and new data hacking technologies, Encryptor already protects data at rest and can cover 250,000 endpoints.

Auditor, pinpointing the real picture

Having the capacity to run on up to 60,000 computers, the clientless Auditor pinpoints the usage USB, FireWire, PCMCIA, PCI, internal storage and WiFi connections on your network. The Auditor searches for information according to Microsoft Active Directory architecture, IP Range and Computer Name and is successfully integrated into the Safend Protector.

WHY SAFEND DPS PROVIDES THE PROTECTIVE EDGE

Understanding where the security challenges are and by introducing proven solutions, Safend DPS protects your facility's endpoints as it monitors, encrypts and updates you on where your data is and who is using it.
Safend DPS is very stable and built comprehensively and once integrated into your network, runs automatically without interrupting daily activities.
Designed as a robust solution for port and device control with a strong anti-tampering mechanism, Safend DPS has built-in compliancy provisions, including for GDPR EU, PCI, HIPAA and SOX.
Safend is already used as a cost-effective data protection solution at major healthcare facilities who have integrated it into their network to protect their sensitive information.