Medigate Medical Device Security Platform (MDSP)

Privacy Impact Assessment

Medigate

July 2021

Table of Contents

1. Executive Summary 3

1.1. Disclaimer 3

1.2. Assumptions, Scope and Limitations 3

1.3. Purpose of the document 4

1.4. Summary 4

2. Findings – Data sensitivity 5

2.1. Data elements 5

2.2. Data sharing 5

2.3. Data flow 5

2.4. Risks and controls 5

3. Findings – Privacy management 7

3.1. Governance 7

3.2. Security 7

3.3. Third parties 8

3.4. User rights 8

3.5. Consent 8

3.6. Training and awareness 9

3.7. Incident handling 9

3.8. Privacy by design 9

4. Record of changes 11

4.1. Revision control 11

5. Appendix A – Data Elements Collected and Processed by Medigate 12

1. Executive Summary

1.1. Disclaimer

In connection with this report (the "report") provided to Medigate by us, we hereby clarify as follows:

- The report was prepared solely in accordance with the engagement letter (the "engagement letter") signed between KPMG and the client and for no other purpose
- The Report was prepared in accordance with the scope agreed with the client.
- KPMG owes the company no duty with respect to, or in connection with the report. The company will rely upon the report entirely at its own risk and KPMG has no liability to the company for any loss or damage suffered or costs incurred by the company arising out of, or in connection with, the provision to the company of the report.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

1.2. Assumptions, Scope and Limitations

The Medigate Medical Device Security Platform ("MDSP") consists of two main components:

- Medigate Collection Server (MCS)
- Medigate Analysis Server (MAS)

This PIA scope is MDSP, where Medigate is the data processor. Almost all data is non-personal and is collected and processed to report on the health, availability, and efficiency of the medical devices connected at the customer's location.

Only incidental personal information, such as an operator's UserID, name of patient's physician, part of the body and its laterality examined, and information about user connection to the device are collected and processed.

1.3. Purpose of the document

The Privacy Impact Assessment (PIA) is a process that identifies what impact a project, initiative or general collection, and use of information might have on the privacy of individuals. A PIA is a point-in-time assessment, and the resultant report and other outputs should be revisited as changes occur to the processes that were originally assessed.
This PIA includes a brief description of the data processed in the MDSP, the privacy impact, and the measures Medigate is taking in order to manage the risks involved.

1.4. Summary

Medigate's Medical Device Security Platform (MDSP) allows biomed and hospitals the ability to understand what is on the network, where it is coming from, and what it is doing. MDSP identifies anomalous behavior, communications and traffic patterns, and the development of effective policies.

We have reviewed the privacy risks regarding MDSP and the privacy and security controls designed to mitigate those risks.

It should be noted that Medigate is a data processor, therefore, some of the personal data-relating processes are the responsibility of the data controller (Medigate customers), such as consent management.

Individuals' personal data in MDSP are limited in nature and the inherent risks resulting is not high. The privacy controls designed and implemented comply with GDPR requirements, relating to the business processes of MDSP.
After reviewing all material GDPR aspects, the privacy risks and implemented controls, any residual risk that we found was minimal. Our impression is that Medigate efforts in implementing GDPR requirements are well managed, resulting in a good level of compliance. Medigate has also appointed a Data Protection Officer (DPO).

One of the main principles of GDPR is Privacy by Design, which means promoting privacy principles throughout product and process development from the start and maintaining this while products and services are developing.

2. Findings – Data sensitivity

2.1. Data elements

The table found in Appendix A describes all of the data fields extracted by Medigate from the collector (server) located at the customer site that is then sent to Medigate analysis servers located in AWS for processing and storing. In addition to this data, Medigate also parses and learns from the metadata of the network activity of the devices (for example, which devices communicate with each other and when). This table addresses the data Medigate extracts from customer information to collect and process.

2.2. Data sharing

Information is not shared with any third-party organizations or individuals.

2.3. Data flow

The MCS is deployed at onsite customer locations to locally ingest packet data through SPAN ports or TAPs and other data sources such as NetFlow and SNMP. The primary function of the MCS is to sniff raw network traffic, filter it and then identify and parse the underlying communication protocols. The MCS then transmits the collected metadata (that does not contain patient information) to the cloud-based MAS. The MAS discovers and identifies the communicating devices, populates all available data attributes for those devices, models a communication profile for the communicating devices, detects anomalies relative to the modelled communication baselines, and carries out all the integration and policy enforcement logic. The MDSP is operated through a web-based Dashboard that is part of the cloud-hosted MAS. The MAS usually runs on a VM in the cloud. For US customers, the analysis server runs on 1-East AWS server farm and has a 1:1 redundant replica within the AWS Seattle server farm.

2.4. Risks and controls

Data processing involves high volume activities. However, the sensitivity of the information collected about individuals is low. None of the data elements are considered special category (GDPR Article 9).

Specific risks and controls:

Main Risks	Key Controls
Disclosure of individuals' data to unauthorized party – internal users	- Access management controls, authentication and authorization mechanisms
Disclosure of individuals' data to unauthorized party – external party	- Application security measures - Operational security including: data center security, server security and network security - Intrusion prevention - EULA - Security monitoring
Processing of personal data without proper need	- Privacy policy - Privacy by Design processes, managed by DPO, including privacy implementation in product development - Privacy assessments
Breach of individual rights	- Data Processing Agreement - Most individual rights are responsibility of data controller - Governance processes by DPO
The organization has not implemented a documented Privacy management framework	- Documented, published and implemented privacy policy - Appointed DPO, responsible for keeping the privacy processes current

3. Findings – Privacy management

3.1. Governance

The development and implementation of the privacy framework is the responsibility of Medigate's Data Protection Officer, Ellen Amsel. This also includes involvement in product development and the following privacy processes:

- developing and providing training regarding privacy and the handling of personal information.
- developing and publishing policy for marketing regarding the collection of customer personal information.
- defining and publishing retention schemes for different types of personal information.
- developing and providing training to development teams regarding Privacy by Design.
- reviewing contracts (usually Exhibits) to ensure Medigate can meet privacy commitments required.
- staying abreast of new privacy regulations to ensure that needed Medigate changes are made, as appropriate
- responding to Data Subject Rights requests in a timely manner
- defining and practicing a privacy incident response process.
- creating and reviewing data flow processes for personal information.

The Medigate Privacy Policy can be found at: https//trust.medigate.io

3.2. Security

The Medigate Information Security Policy can be found at: https//trust.medigate.io

Medigate is ISO 27001 certified, and has implement security controls in the following areas:

- Physical security
- Operational security
- Network security
- Intrusion prevention
- Application security
- Access control
- Asset management
- Backup controls
- Privacy management
- Risk management and compliance

A current copy of Medigate's ISO 27001 certificate can be found at: https//trust.medigate.io

A copy of the Statement of Applicability, that defines which ISO 27001 controls have been implemented and validated, can be found at: https//trust.medigate.io trust

3.2.1. Physical security

The Medigate collection server (MCS), located at the customer's site, relies on the physical security controls in place at the customer location.

The Medigate analysis server (MAS), located at the Amazon Web Services (AWS) datacenter, relies on the physical controls implemented by AWS at the AWS datacenter.

3.3. Third parties

Medigate does not share personal data with any third parties.

According to the Medigate Privacy Policy, "Whenever the Company uses a third-party supplier or sub processor to process personal data on its behalf, the information security officer will ensure that this sub-processor will provide security measures to safeguard personal data that are appropriate to the associated risks. For this purpose, a data processing agreement shall be implemented.

The Company contractually will require the supplier or business associate to provide the same level of personal data protection. The supplier or business associate must only process personal data to carry out its contractual obligations towards the Company or upon the instructions of the Company and not for any other purposes."

3.4. User rights

User rights are addressed by Medigate's Privacy Policy.

"Data subjects have the rights to access, erased and portability their personal data. Those data subjects access requests will be treated as described in "Data subject access request procedure."

3.5. Consent

Consent is managed by the customer, who is the data controller.

3.6. Training and awareness

Medigate is managing a privacy awareness training program, as well as a security awareness training program. Additionally, specialized Privacy by Design training has been conducted specifically for GDPR.

3.7. Incident handling

Medigate has developed and implemented an incident response and notification process. Procedures include breach notification policy and the involvement of the DPO in case of a data breach as determined in Medigate's Privacy Policy:

"When the Company learns of a suspected or actual personal data breach, Information security officer will perform an internal investigation and take appropriate remedial measures in a timely manner, according to the Data Breach notification procedure. Any further acts will be done as described in the Data Breach notification procedure."

3.8. Privacy by design

Medigate has implemented a Privacy by Design processes, which involves the DPO and addresses privacy concerns from the beginning of product development and through change management.

Privacy by design is addressed in the Medigate Privacy Policy (article 4.3.2):

"The information security officer will be involuntarily involved in new projects / products developments in the company and will input the privacy and personal data protection aspects to these processes."

3.8.1. Data minimization

The information collected by MDSP platform (specific data elements listed in Appendix A) is limited to the information necessary, relevant and proportionate to the purposes of the system use. Only personal data which is necessary for processing is collected. Data minimization is addressed by the Medigate Privacy Policy:

"The Company strive to collect the least amount of personal data possible. If personal data is collected from a third party, the CEO and the Information security officer will ensure that the personal data is collected lawfully. "

3.8.2. Data retention

3.8.2.1. Operational data used by Medigate

Medigate has established data retention requirements for logs and other operational data. In general, this data is retained for 90 days.

3.8.2.2. Customer data

The Medigate platform allows for the retention of historical data to support customer auditing needs. The data retention period for this data is defined by the customer according to support their own internal requirements.

3.8.2.3. Medigate Privacy Policy

As stated in the Medigate Privacy Policy, “Personal data will be kept for no longer than is necessary for the purposes for which the personal data are processed. “

4. Record of changes

Type of Information	Document Data
Document Title:	Medigate platform Privacy Impact Assessment
Document Owner:	Ellen Amsel, Head of Information Security and Privacy & DPO
Approved by:	Jonathan Langer, CEO
Release date:	July 18, 2021
Reviewed & Revised:	December 15, 2021

4.1. Revision control

Version Number	Nature of Change	Date Approved
1.0	Initial version	July 18 ,2021
2.0	Reviewed and updated	October 28, 2021
3.0	Reviewed and updated	December 15, 2021

5. Appendix A – Data Elements Collected and Processed by Medigate

Field Name	Description	Comments
DICOM		
id	User or equipment generated identifier of that part of a Procedure that has been carried out within this step	
description	MPPS step description	
modality	Type of equipment that originally acquired the data used to create the images in this Series.	
ae_title	Application Entity Title. A unique name that is given to imaging devices, servers and IW. Usually it is unique for a combination of IP address and port number.	
protocol_code_value	Identified or the coded entry	
protocol_coding_scheme	The identifier of the coding scheme in which the Coded Entry is defined	
protocol_code_meaning	A text that conveys the meaning of the Coded Entry	
start_datetime	The time when the procedure started	
end_datetime	The time when the procedure was finished	

Field Name	Description	Comments
DICOM Procedure		
accession_number	A RIS generated number that identifies the order for the Study.	
code_value	Identified or the coded entry	
coding_scheme	The identifier of the coding scheme in which the Coded Entry is defined	
code_meaning	A text that conveys the meaning of the Coded Entry	
DICOM Study		
study_uid	A unique uid is generated for each study	
referring_physicians_name	Name of the Patient's referring physician	
station_name	User defined name identifying the machine that produced the imaging procedure	
location	Location of where the scheduled procedure took place. Usually it is the name(station name) or part of the name of the device	
primary_device_uid	Unique medigate uid that is given for each device. Primary indicates that this device is considered as the main device (among other related devices, for example by multiple NICs).	

Field Name	Description	Comments
prefix_id	A prefix name. The Prefix is part of the series/image UID.	
related_series_number	Number of series that are in each study	
related_instances_number	Total number of images in each study	
DICOM Series		
series_uid	Unique identifier of the Series	
body_part	text description of the part of the body examined	
laterality	Laterality of (paired) body part examined (left ot right)	
operators_name	Name(s) of the operator(s) supporting the examination	
protocol_name	User-defined description of the conditions under which the Series was performed	
performing_physicians_name	Name of the physician(s) administering the Series	
manufacturer	Manufacturer of the device	
station_ae_title	Application Entity Title of the device identified	
scheduled_station_ae_title	The AE title of the modality on which the Scheduled Procedure Step is	

Field Name	Description	Comments
	scheduled to be performed	
performed_station_ae_title	AE title of the modality on which the Performed Procedure Step was performed	
implementation_class_uid	Identifiers that are used in DICOM protocol.	
institution_address	Mailing address of the institution where the equipment that produced the imaging is located	
institution_name	Institution where the equipment that produced the imaging is located	
institutional_department_name	Department in the institution where the equipment that produced theimaging is located	
DICOM Image		
serial_number	Manufacturer's serial number of the equipment that produced the imaging	
acquisition_number	A number identifying the single continuous gathering of data over a period of time that resulted in this image	
sop_class_uid	Uniquely identifies the SOP Class	
instance_datetime	The time that DICOM instance was created	

Field Name	Description	Comments
content_datetime	The time that the image was formed from acquisition "The date the image pixel data creation started	
acquisition_datetime	The time that acquisition that resulted in the image occurred. "The date the acquisition of data that resulted in this image started	
pixel_data_characteristics	Whether the image is from ORIGINAL or DERIVED pixel source	
patient_examination_characteristics	Whether the image was created from examination and thus PRIMARY or created after examination and thus SECONDARY	
is_quality_control	Whether or not this image is a quality control or phantom image	
contains_burned_in_annotation	Whether or not the image contains sufficient burned-in annotation to identify the patient and date the image was acquired.	
contains_recognizable_visual_features	Whether or not the image contains sufficiently recognizable visual features to allow the image or a reconstruction from a set of images to identify the Patient	
manufacturers_model_name	Manufacturer's model name of the equipment that produced the imaging	
source_serial_number	Identifier for the (radiation) Source Instance	

Field Name	Description	Comments
image_type	Image identification characteristics (ORIGINAL/DERIVED/ PRIMARY/SECONDARY etc)	
Device Information		
mac	MAC address	
ip	IP address	
vlan	VLAN	
protocols	Network communication protocols	
hostnames	Hostnames	
dns_requests	Domains addressed by DNS protocol	
first_seen	First seen by Medigate	
last_seen	Last seen by Medigate	
online	Status in the network	
since	Last time the device went online	
connection_type	E.g. ethernet, serial	
ip_assignment	Static or dynamic (DHCP lease)	

Field Name	Description	Comments
wired	Wired or wireless network connection	
location	Physical location indicated by wireless connection	
device_type_family	Device type categories	
vendor	Device manufacturer	
model	Device model	
serial_number	Serial number	
hw_version	Hardware version	
sw_version	Software version	
local_names	Similar to hostname, the device name identifier is extracted from protocol traffic	
gateways	Any network communication gateway for that specific device	
os_name	Operating system name	
os_version	Operating system version	
os_revision	Operating system revision	
fda_class	FDA Class 1, 2, or 3	

Field Name	Description	Comments
infected	The infection status of the device, extracted from MDM or EDR integrations	
ad_distinguished_name	The Active Directory distinguished device name extract from Microsoft Active Directory integration	
ad_description	The Active Directory device description extracted from the Microsoft Active Directory integration	
has_segmentation_information	Does the device have network segmentation information in Cisco ISE	
authentication_method	The device's Authentication Method extracted from Cisco ISE integration	
authorization_profile	The device's Authorization Profile extracted from Cisco ISE integration	
endpoint_policy	The device's Endpoint Policy extracted from Cisco ISE integration	
identity_group	The device's Identity Group extracted from Cisco ISE integration	
wlc_location	The location of the Wireless LAN Controller that control access points on the network	
logical_group	The device's Logical Profile extracted from Cisco ISE integration	
posture_status	The state of the device as reported in Posture service extracted from Cisco	

Field Name	Description	Comments
	ISE integration	
identity_store	A property extracted from Cisco ISE integration	
security_group	The device's Security Group extracted from Cisco ISE integration	
wlc_name	The name of the Wireless LAN Controller that controls access points on the network	
user_name	The username used by the device to authenticate to the network using Radius/802.1x. This data is extracted from NAC integration	
mdm_ownership	The ownership of the mobile device incorporated in the MDM platform. Extracted from MDM integrations	
mdm_compliance_status	The compliance status of the mobile device incorporated in the MDM platform. Extracted from MDM integrations	
mdm_enrollment_status	The enrollment status of the mobile device incorporated in the MDM platform. Extracted from MDM integrations	
edr_is_up_to_date	Determines whether the endpoint security application installed on the device is up-to-date (numeric - 0/1)	
edr_is_up_to_date_text	Determines whether the endpoint security application installed on the device is up-to-date (numeric values -	

Field Name	Description	Comments
	True/False)	
edr_last_scan_time	Last time scanned by EDR/AV	
battery_level	The battery status of the device. Relevant to Infusion Pumps only	
alaris_dataset_name	For Alaris devices, the current dataset name, extracted from the Alaris DCMP traffic.	
alaris_pending_dataset_name	For Alaris devices, the pending dataset name, extracted from the Alaris DCMP traffic.	
alaris_dataset_updated	For Alaris devices, whether the current dataset name is up-to-date, extracted from the Alaris DCMP traffic.	
dhcp_fingerprint	An identifier for a DHCP lease requester	
VLANs		
vlan_qualifier	Used to distinguish between different VLANs who share the same VLAN ID	Generated by Medigate
vlan_name	VLAN name	
vlan_description	VLAN description	
is_guest_vlan	Flag whether the VLAN is configured as Guest or Corporate	

Field Name	Description	Comments
network	VLAN Subnet	Generated by Medigate
User Data		
(user) first_seen	First seen of the user connection to the device	*This is for the device + user*
(user) last_seen	Last seen of the user connection to the device	*This is for the device + user*
domain	User's domain	
username	Username	
note	Note	Mostly null
Patches and Applications		
hotfix_id	The identifier of a given hotfix / patch / update	
installed_by	The user that performed the hotfix installation	Can be local user, domain user, user SID etc.
installed_date	Hotfix installation date	
app_name	Application name	
app_version	Application version	
app_vendor	Application vendor	

Field Name	Description	Comments
app_public_id	A globally unique application identifier	Like MacOS's "Bundle Identifier"
windows_guid	A globally unique application Windows GUID	Also known as an "IdentifyingNumber"
Location and Access Point		
switch_ip	Switch IP address	
switch_group_name	Switch group name	
switch_port	Switch port	
switch_port_type	Gigabit Ethernet / Fast Ethernet	
switch_mac	Switch MAC address	
switch_location	Location of the switch	
switch_device_type	Vendor and model of the switch	
switch_port_description	Switch port name	
bssid	MAC address of the AP	
ap_name	AP name	
ap_ssids	AP SSIDs	

Field Name	Description	Comments
ap_location	AP location	
campus_name	AP location information	
building_name	AP location information	
floor_name	AP location information	
floor_image_path	Path to floor image file	
floor_image_taken_from	Integration source	
floor_height	Height of floor image	
floor_width	Width of floor image	
position_x_in_image	Location on X axis	
position_y_in_image	Location on Y axis	
Additional Protocol Data		
HTTP Header - User Agent	HTTP User Agent Sent by the device	*Limited to 20 per device*
HTTP Header - Start Line	HTTP Start Line sent by the Device	*Limited to 20 per device*
HTTP Header - Server	HTTP Server Identification sent by the Device	*Limited to 20 per device*
HTTP Header - Title	HTTP Title sent by the Server to a	*Limited to 20 per device*

Field Name	Description	Comments
	Device	
DNS Request - Domain	The Domain requested by a Device	
TDS - Database Name	MSSQL Database Name from TDS protocol	
TDS - Table Name	MSSQL Table Name from TDS protocol	
TLS - Certificate	TLS Certificate as sent by the Server - CN and Thumbprint	
SNMP - OID	SNMP Request value	
SNMP - Response	SNMP Response value	
MDNS - Values	Value advertised in MDNS Protocol	
SIP - User Agent	SIP User Agent sent by the device (VoIP)	
SIP - Server	SIP Server Identification (VoIP)	
H225 - Manufacturer Code	Manufacturer Code sent by the device (VoIP)	
H225 - Product ID	Product ID sent by the device (VoIP)	
RTSP - User Agent	RTSP User Agent Sent by the device (VoIP)	

Field Name	Description	Comments
RTSP - Realm	RTSP Realm (VoIP)	
RTSP - Server	RTSP Server Identification (VoIP)	
WSD - Scope	Scope advertised in WSD Protocol	
WSD - Type	Type advertised in WSD Protocol	
Browser - Comment	Comment sent by device in Windows Browser protocol	
BACNET - Vendor ID	Vendor ID sent by the device (Building Automation)	
BACNET - Device ID	Device ID sent by the device (Building Automation)	
FTP - Username	FTP Username sent by device to server	
FTP - Server Banner	Banner Sent by FTP Server	
HL7 - MSH Header	HL7 MSH Header fields: MSH.3 - Sending Application MSH.4 - Sending Facility MSH.5 - Receiving Application MSH.6 - Receiving Facility	
NMF - Service Name	Service advertised in NMF Protocol	
LIS2A - H Record	# --- Header record (H) --- # 1 delimiter definition	

Field Name	Description	Comments
	# 2 message control id # 3 access password # 4 sender name/id # 9 receiver id	